993397

[19]中华人民共和国专利局

[51]Int.Cl[6]
G06F 12/14
G06F 3/06 G11B 20/10

[12]发明专利申请公开说明书

[21]申请号 96190821.1

[43]公开日 1997年9月10日

[11]公开号 CN 1159235A

[22]申请日 96.6.18

[30]优先权

[32]95.6.30 [33]JP[31]166698/95

[32]95.6.30 [33]JP[31]187967/95

[86]国际申请 PCT/JP96/01675 96.6.18

[87]国际公布 WO97/02531 日 97.1.23

[85]进入国家阶段日期 97.3.27

[71]申请人 索尼公司

地址 日本东京都

[72]发明人 佐古曜一郎 川鸣功 栗原章
大泽义知 志和英男

[74]专利代理机构 柳沈知识产权律师事务所

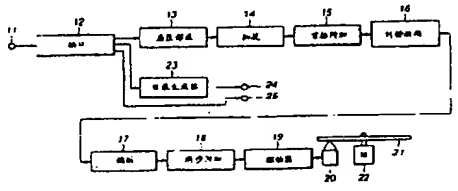
代理人 马莹

权利要求书 7 页 说明书 19 页 附图页数 29 页

[54]发明名称 数据记录方法及装置、数据记录媒体与数据重现方法及装置

[57]摘要

输入至少在下述电路之一被加密：扇区形成电路13，加扰电路14，首标附加电路15，纠错编码电路16，调制电路17和同步附加电路18，上述电路用于对输入数据进行处理以形成记录信号。不仅所述电路中用于加密的密钥本身，而且有关已使用了哪一个电路的信息也成为用于加密的密钥。这就用简化的结构实现了难于解码的加密。



权 利 要 求 书

1. 一种数据记录方法，包括：

以预置的数据卷为单位划分输入数字数据的扇区形成步骤；

附加首标于已分成扇区的数字数据的首标附加步骤；

附加纠错代码于已附有首标的数字数据的纠错编码步骤；

根据预置的调制系统来调制已纠错编码的数字数据的调制步骤；

附加同步模式于已调制数字信号的同步附加步骤；和

在记录媒体上记录已附加有同步模式的数字信号的记录步骤；

其中

至少在所述的扇区形成步骤，首标附加步骤，纠错编码步骤，调制步骤和同步附加步骤之一中对输入数据加密并输出所得的已加密数据。

2. 如权利要求 1 所述的数据记录方法，还包括在所述扇区形成步骤中对所述分成扇区的数字数据实施随机化或在所述首标附加步骤中对所述附加有首标的数字数据实施随机化以消除相同模式的加扰步骤；

其中，至少在所述的扇区形成步骤，首标附加步骤，纠错编码步骤，调制步骤，同步附加步骤和加扰步骤之一中对输入数据加密并输出所得的加密数据。

3. 如权利要求 1 所述的数据记录方法，其中，在所述的加密中使用的多种密钥信息根据预置的定时被设置和切换。

4. 如权利要求 1 所述的数据记录方法，其中，在所述的扇区形成步骤、首标附加步骤、纠错编码步骤、调制步骤和同步附加步骤中哪一步骤已进行了加密被用作密钥信息。

5. 如权利要求 1 所述的数据记录方法，其中，在所述纠错编码步骤中经纠错编码处理的数据中，至少与用于加密的密钥信息相符的部分被数据转换所处理。

6. 如权利要求 1 所述的数据记录方法，其中所述的纠错码是乘积码。

7. 一种数据记录装置，包括：

扇区形成装置，用于以预置的数据卷为单位划分输入数字数据；

首标附加装置，用于附加首标于所述扇区形成装置所输出的数字数据；

纠错编码装置，用于附加纠错代码于所述首标附加装置所输出的数字数

据;

调制装置，用于调制所述首标附加装置输出的数字数据;

同步附加装置，用于附加同步模式于所述调制装置所输出的数字信号;和

记录装置，用于在记录媒体上记录所述调制装置所输出的数字信号；其中

至少在所述的扇区形成装置、首标附加装置、纠错编码装置、调制装置和同步附加装置之一中对输入加密并输出所得到的加密数据.

8. 如权利要求 7 所述的数据记录装置，还包括加扰装置，用于对被所述扇区形成装置划分成扇区的数字数据或对被所述首标附加装置附加首标的数字数据实施随机化以消除相同模式;

其中，至少在所述的扇区形成装置、首标附加装置、纠错编码装置、调制装置、同步附加装置和加扰装置之一中对输入加密并输出所得到的加密数据.

9. 如权利要求 8 所述的数据记录装置，还包括数据转换装置，用于至少对在纠错编码时被处理的又与用于加密的密钥信息相符合的部分数据进行数据转换.

10. 一种数据记录媒体，其上带有记录数据，所述记录数据通过把输入数字数据以预置数据卷为单位形成为扇区、通过首标附加附加首标于每一扇区、并且通过纠错和编码、根据预置调制系统调制和附加同步模式对所述形成扇区并附加有首标的结果数据进行处理而获得，被处理的结果数据在形成扇区、附加首标、纠错和编码、调制或附加同步模式时被加密.

11. 一种数据重现方法，包括:

同步分离步骤，用于从数据记录媒体读出的数字信号中分离同步信号;

根据预置解调系统对从同步信号分离出来的数字信号解调的解调步骤;

对已解调数字数据进行纠错和解码的纠错解码步骤;

将已纠错和解码的数字数据分解成预置扇区的扇区分解步骤；和

分离被分解成扇区的数字数据的扇区结构中的首标部分的首标分离步骤;

其中，输入已经在至少与所述同步分离步骤、解调步骤、纠错解码步骤、

扇区分解步骤或首标分离步骤之一相关联的记录步骤中被加密；和其中

输入在与记录时已经进行加密的记录步骤相关联的重现步骤中被解密；

12. 如权利要求 11 所述的数据重现方法，还包括对在记录时被加扰的数字数据进行解扰的解扰步骤，所述数字数据已在扇区分解步骤中被分解为扇区或在首标分离步骤中从首标中分离出来；

其中，输入已经在至少与同步分离步骤、解调步骤、纠错解码步骤、扇区分解步骤首标分离步骤或解扰步骤之一相关联的记录步骤中被加密；和其中

输入在与记录时已经进行加密的记录步骤相关联的重现步骤中被解密.

13. 一种数据重现装置，包括:

同步分离装置，用于从数据记录媒体读出的数字信号中分离同步信号；

解调装置，用于根据预置的解调系统对所述同步分离装置输出的数字信号进行解调；

纠错解码装置，用于对所述解调装置输出的数字数据进行纠错和解码；

扇区分解装置，用于将所述纠错解码装置输出的数字数据分解成预置扇区；和

首标分离装置，用于分离由所述扇区分离装置输出的数字数据的扇区结构中的首标部分；

其中，输入已经在至少与同步分离装置、解调装置、纠错解码装置、扇区分解装置和首标分离装置之一相关联的记录步骤中进行加密；和其中

输入在与记录时已经进行加密的记录步骤相关联的重现装置中被解密.

14. 如权利要求 13 所述的数据重现装置，还包括对在记录时加扰的数字数据进行解扰的解扰装置，所述数字数据被所述扇区分解装置或所述首标分离装置输出；

其中，输入已经在至少与所述的同步分离装置、解调装置、纠错解码装置、扇区分解装置、首标分离装置和解扰装置之一相关联的记录装置中被加密；和其中

输入在与记录时已经进行加密的记录装置相关联的重现装置中被解

密.

15. 一种数据记录方法，用于对输入数字数据纠错和编码和在记录媒体上记录结果数据，其中，至少对在纠错和编码时被处理的又与用于加密的密钥信息相符合的部分数据进行数据转换处理.

16. 如权利要求 15 所述的数据记录方法，其中所述的数据转换至少通过以下操作之一来实现：对数据和密钥信息的逻辑处理，使用密钥信息来进行的替换或置换功能处理.

17. 如权利要求 15 所述的数据记录方法，其中利用所述数据转换处理的数据总数随加密中遇到的难度而变化.

18. 一种数据记录装置，用于对输入数字数据进行纠错编码和在记录媒体上记录结果数据，包括：

输入装置，用于输入供加密用的密钥信息；和

数据转换装置，用于响应于从所述输入装置输入的密钥信息而至少对在纠错和编码过程中被处理的部分数据进行数据转换.

19. 一种数据记录媒体，其上记录有信号，所述信号通过至少对输入数字数据的纠错和编码时被处理的又与用于加密的密钥信息相符的部分数据进行转换而获得.

20. 一种用于重现被纠错和编码处理并被记录在记录媒体上的信号的方法，其中，

至少对纠错和编码时被处理的又与用于加密的密钥信息相符合的部分数据进行数据转换处理，和其中，

在与纠错和编码相对应的纠错和解码时被处理的又与用于加密的密钥信息相符合的数据被进行与数据转换相对应的数据反转换处理.

21. 一种用于重现被纠错和编码处理并被记录在记录媒体上的信号的装置，包括：

密钥信息输入装置，用于输入密钥信息，所述密钥信息用于加密在纠错和编码时被处理的和被数据转换处理的特定数据；和

纠错和解码装置，用于进行与纠错和编码相对应的纠错和解码，所述纠错和解码装置执行与所述数据转换相反的操作，即对从密钥信息输入装置输入的、与用于加密的密钥信息相符合的数据进行纠错和解码.

22. 一种数据记录方法，其中输入数据被用于记录的信号处理所处理并

被记录在记录媒体上的预置记录区域内，其中，

通过使用预置的密钥信息对数据加密，和其中，

把记录在所述记录媒体上不同于记录区域的区域内的信息至少作为用于加密的密钥信息的一部分来使用.

23. 如权利要求22所述的数据记录方法，其中，至少把下述识别信息之一作为所述的密钥信息来使用：记录媒体专用的识别信息，记录设备专用的识别信息，记录媒体的生产设备专用的识别信息，生产商/销售商识别信息，地区信息和从外部提供的识别信息.

24. 一种数据记录装置，在所述的数据记录装置中，输入数据被用于记录的信号处理所处理并被记录在记录媒体上的预置记录区域内，其中，

通过使用预置的密钥信息对数据加密，和其中，

把记录在不同于所述记录媒体上记录区域的区域中的信息至少作为用于加密的密钥信息的一部分来使用.

25. 一种数据记录媒体，在所述的记录媒体上，通过使用至少其一部分记录在与数据记录区域不同区域中的密钥信息来进行加密而获得的数据被记录在所述的数据记录区域内.

26. 一种数据重现方法，在所述的数据重现方法中，对从数据记录媒体上的数据记录区域读出的数字信号进行用于重现的信号处理，所述数字信号在记录时已经被加密，其中

通过使用记录在与所述记录媒体上数据记录区域不同区域中的信息进行解密，所述信息至少被作为用于加密的密钥信息的一部分.

27. 如权利要求26所述的数据重现方法，其中，至少下述识别信息之一被用作密钥信息：记录媒体专用的识别信息、记录设备专用的识别信息、记录媒体的生产设备专用的识别信息，生产商/销售商识别信息，地区信息和从外部提供的识别信息.

28. 一种数据重现装置，在所述数据重现装置中，对从数据记录媒体上的数据记录区域读出的数字信号进行用于重现的信号处理，所述数字信号在记录时已被加密，其中

通过使用记录在与所述记录媒体上数据记录区域不同的区域中的信息进行解密，所述信息至少被作为用于加密的密钥信息的一部分.

29. 一种数据记录方法，包括：

以预置数据卷为单位划分输入数字数据的扇区形成步骤;

加扰步骤，用于对划分成扇区的数字数据进行加扰;

附加首标于被加扰的数字数据的首标附加步骤;

附加纠错代码于已附加首标的数字数据的纠错编码步骤;

根据预置调制系统对已纠错编码的数字数据进行调制的调制步骤;

附加同步模式于已调制的数字信号的同步附加步骤；和

记录已附加同步模式的数字信号的记录步骤;

其中，根据用于加密的密钥信息来至少改变加扰步骤初始值或生成多项式这二者中的一个。

30. 一种数据记录装置，包括:

扇区形成装置，用于以预置数据卷为单位划分输入数字数据;

加扰装置，用于对从所述扇区形成装置输出的数字数据进行加扰处理，在所述加扰中，根据用于加密的密钥信息来至少改变预置值和生成多项式这二者中的一个;

首标附加装置，用于附加首标于从所述加扰装置输出的数字数据;

纠错编码装置，用于附加纠错代码于所述加扰装置输出的数字数据;

调制装置，用于根据预置调制系统对所述纠错编码装置输出的数字数据进行调制;

同步附加装置，用于附加同步模式于所述调制装置输出的数字信号；和

记录装置，用于记录从所述同步附加装置输出的数字信号.

31. 一种数据记录媒体，其上记录有信号，所述信号通过以预置数据卷为单位将输入数字数据形成扇区而获得，如此形成扇区的数据被进行加扰处理，所述加扰处理中，初始值和生成多项式这二者中至少有一个响应于用于加密的密钥信息而被改变，加扰后得到的数据附加有首标，并且根据预置调制系统对带有首标的结果数据进行纠错编码和调制处理.

32. 一种数据重现方法，包括:

将同步信号从数据记录媒体上读出的数字信号分离出来的同步分离步骤;

根据预置调制系统对从同步信号分离出来的数字信号进行解调的解调步骤;

对从解调获得的数字数据进行纠错和解码的纠错解码步骤;

对已纠错和解码的数字数据进行分解的扇区分解步骤;

分离被分解成扇区的数字数据的扇区结构的首标部分的首标分离步骤; 和

根据用于记录的密钥信息, 通过至少改变初始值或生成多项式这二者之一对已与首标分离的数字数据进行解扰的解扰步骤.

33. 一种数据重现装置, 包括:

同步分离装置, 用于将同步信号从数据记录媒体上读出的数字数据分离出来;

解调装置, 用于根据预置调制系统对从所述同步分离装置输出的数字信号进行解调;

纠错和解码装置, 用于对从所述解调装置获得的数字数据进行纠错和解码;

扇区分解装置, 用于分解从所述纠错和解码装置输出的数字数据;

首标分离装置, 用于分离从所述扇区分解装置输出的数字数据的扇区结构中的首标部分; 和

解扰装置, 用于根据用于记录的密钥信息, 通过至少改变初始值或生成多项式这二者之一, 对从所述首标分离装置输出的数字数据进行解扰.

说　明　书

数据记录方法及装置、数据记录媒体与数据重现方法及装置

本发明涉及用于防止拷贝或禁止未经许可而使用的和用于交费系统的一种数据记录方法及装置、一种数据记录媒体与一种数据重现方法及装置.

近来，随着数字记录(记录用的、可记录的、或已记录的)媒体能力的增加和开始广泛使用，防止拷贝或禁止未经许可的使用也越来越重要了．这就是说，由于计算机数据能够被轻易的拷贝而产生同原始数据同样的数据，同时，数字音频数据或数字视频数据能够通过拷贝或转录被复制而不会损坏，而因此未经许可的拷贝屡见不鲜.

为了避免数字音频或视频数据的未经许可的拷贝，已知有一种被称为“串行拷贝管理系统”(SCMS)或“拷贝生成管理系统”(CGMS)的标准．由于这些系统在记录数据的特定部分设置了禁止拷贝的标志，因此出现了能够通过转储拷贝即对数字双层信号整体的拷贝来提取数据的问题.

对于计算机数据，将文件内容本身加密和只允许正式注册的用户使用，例如象日本专利第昭－60－116030号所公开的那样，也付诸实施了．将这种用法与一个系统相结合，该系统发行一种具有加密记录信息的数字记录媒体作为信息流通的一种形式，用户要交付费用以获取他或她需要的对信息解密的密钥．对于上述的系统，需要一种用于加密的简单实用的技术.

鉴于上述的技术背景，本发明的一个目的是提供一种数据记录的方法及装置，一种数据记录媒体与一种数据重现的方法及装置，从而能够通过简化的结构来实现加密、通过简化的结构来实现禁止拷贝或未经许可的使用，使得解密困难并且能够容易地控制相关的装置或加密的深度.

本发明的记录方法的特点在于输入数据至少在下列步骤之一中被加密：将输入数字数据以预置数据卷为单位进行划分的扇区形成步骤，附加首标的步骤，纠错与译码的步骤，根据预置的调制系统实施调制的调制步骤，或附加同步模式的同步附加步骤．实施随机化以消除相同模式的加扰步骤可以包括在可用于加密的这些步骤中.

上述的数据记录方法能够应用于数据记录装置.

本发明的数据重现方法的特点在于，在按照上述数据记录方法记录的数据记录媒体的重现中，输入数据至少已经在下列步骤之一所对应的记录步骤中被加密：同步分离步骤，解调步骤，纠错与译码步骤，扇区分解步骤和首标分离步骤；还在于输入数据在与用于加密的记录步骤相对应的重现步骤中被解密．对用于记录的加扰进行解扰的解扰步骤可以包括在可用于解密的这些步骤之中.

上述数据重现方法能够应用于数据重现装置.

使用本发明的数据记录方法，通过使用预置的密钥信息和使用被写在不同于记录媒体的数据记录区域的区域中的信息作为用于加密的密钥信息的一部分对数据加密来实现上述的目的．上述方法能够应用于数据记录装置和应用于数据记录媒体.

本发明的数据重现方法的特点还在于，当重现在记录过程中被加密的数字信号时，通过使用密钥信息来实现解密，所述密钥信息的至少一部分被写入与记录媒体的数据记录区域不同的区域.

上述方法能够应用于数据重现装置.

本发明的数据记录方法的特点还在于根据用于记录的密钥信息来至少改变加扰步骤的初始值和生成多项式这二者中的一个.

本发明的数据重现方法的特点还在于根据用于记录的密钥信息来至少通过改变初始值和生成多项式这二者中的一个来进行解扰.

输入数字数据以预置数据卷为单位的形式划分成扇区，并且结果数据通过首标附加，纠错与编码，使用预置调制系统进行调制和附加记录媒体上的用于记录的同步模式来进行处理．通过至少在上述步骤之一对输入数据加密，完成加密的某一特定的步骤也成为加密的密钥，因此增加了解密的难度.

至少一部分用于加密的密钥信息被写入不同于记录媒体上的记录区域的区域．这部分密钥信息在重现时被读出并用于解密．由于密钥信息不完全等同于记录媒体上数据记录区域中的信息，使得解密的难度增加了.

在加扰期间，根据用于加密的密钥，至少改变生成多项式和初始值这二者中的一个．加扰的目的在于随机化，以消除数据串中相同的模式．任何一般的加扰都可用于加密.

图 1 是本发明数据记录装置的第一实施例结构的简要方框图.

图2是在扇区形成电路中实现偶字节和奇字节交错的说明性结构的方框图.

图3表示偶字节和奇字节的交错.

图4是加扰器的一个例子.

图5说明加扰器的预置值的一个例子.

图6说明具有可变生成多项式的加扰器的一个例子.

图7说明扇区格式的一个例子.

图8说明在扇区内同步区域进行加密的一个例子.

图9所示的是扇区内首标区域的一个例子.

图10所示的是纠错编码电路的概略结构.

图11所示的是纠错编码电路的详细结构.

图12所示的是纠错编码电路的另一例.

图13所示的是在调制电路中的加密的一个例子.

图14所示的是附加在已调制信号上的同步字的一个特定的例子.

图15所示的是在同步附加电路中加密的一个例子.

图16所示的是数据记录媒体的一个例子.

图17所示的是本发明数据重现装置的第一实施例的简要结构的方框图.

图18所示的是通过解调电路进行解密的一个例子.

图19所示的是纠错解码电路的一个例子的简要结构图.

图20所示的是纠错解码电路的一个例子的详细结构图.

图21所示的是纠错解码电路的另一个例子.

图22所示的是解扰电路的一个例子.

图23所示的是加扰器的另一个例子.

图24所示的是图23所示的加扰器的预置值的一个例子.

图25表示扇区格式的另一例.

图26是说明图25所述的扇区格式形式的一个扇区首标区域的一个例子.

图27是纠错编码电路的另一个例子的方框图.

图28是说明把乘积码作为纠错码的一个特定的例子.

图29是说明扇区信号格式的一个例子.

图 30 是说明附加在已调制信号上的同步字的另一个特定例.

图 31 是说明在同步附加电路中进行加密的另一例.

图 32 是说明纠错解码电路的另一个例子的方框图.

下面结合附图详细说明本发明的优选实施例.

图 1 扼要地表示本发明的第一实施例.

在图 1 中，数字数据，例如对模拟音频或视频信号或计算机数据进行数字转换而获得的数据，被传送到输入端 11．输入数字数据通过接口电路 12 被送至扇区形成电路 13，以预置数据卷(如 2048 字节)为单位来形成扇区．如此形成扇区的数据被送至加扰电路 14 进行加扰．对于加扰而言，由于输入数据被随机化，因此相同字节样式将不会连续地产生，也就是说通过随机化的方式，消除了相同的模式，使得信号能够被恰当地读取和记录．经过加扰或随机化的数据被送至首标附加电路 15，排列在每个扇区前端的首标数据在这里被附加，并且所得到的数据被送至纠错编码电路 16．纠错编码电路 16 延迟数据，并产生校验码以附加所生成的校验码．下一个电路，即调制电路 17，将 8 位数据根据预置的调制规则转换为 16 通道位的调制数据，并将所得到的已调制数据送至同步附加电路 18．同步附加电路 18 以预置数据卷为单位附加一违反上述预置调制系统调制规则的同步信号，即被称作不规则模式的同步信号，并且通过一驱动电路，即驱动器 19，将所得到的同步信号传送至记录头 20．记录头 20 执行光学的或磁光的记录和存在记录媒体上记录已调制信号．盘状记录媒体 21 通过主轴电机 22 作旋转运动.

加扰电路 14 并非必需的．而且加扰电路 14 可以插在首标附加电路 15 之后，对带有附加首标的数字数据进行加扰．带有附加首标的数字数据可以送至纠错编码电路 16．

应当注意的是，在扇区形成电路 13，加扰电路 14，首标附加电路 15，纠错编码电路 16，调制电路 17 和同步附加电路 18 中，至少配置其中之一来加密输入数据并输出经过加密的信号．最好是用两个或两个以上的电路进行加密．用于加密的密钥信息的至少一部分使用被写入与记录媒体 21 的数据记录区域不同的区域的识别信息，如媒体本身的识别信息，生产商识别信息，销售商识别信息，记录装置或编码器本身的识别信息，媒体生产设备(如切割机或冲压机)本身的识别信息，地区信息(如国家代码)或从外部提供的识别信息．这些被如此写入与记录媒体的数据记录区域不相同区域的识别信息通过

目录(TOC)生成电路 23，从接口电路 12 送至端子 24 和直接从接口电路 12 送至端子 25．从端子 24、25 输出的识别信息被用作加密的密钥信息的一部分．电路 13 至 18 的至少一个，最好是二个或更多个电路使用该密钥信息对输入数据加密．从端子 24、25 输出的识别信息被作为适当的信息送至用于在记录媒体 21 上作记录的记录头 20．

在这种情况下，电路 13 至 18 中哪一个电路执行了加密代表了一种选择，并且被认为是用来在重现过程中产生正常重现信号所需的密钥．这就是说，如果加密已在所述电路之一进行，就需要在六种选择中择其一．而如果加密已在所述电路的两个中进行时，则需要在相应于从六个电路中选择两个电路的组合数字，即在 15 种选择中择其一．如果加密有可能在 6 个电路 13 至 18 中的一至六个电路中进行，则可供选择的种数将会进一步增长，使得采用试凑法很难找到该组合，因此起到了加密的作用．

用于加密的密钥信息可以根据预置的定时，例如在扇区的基础上，来进行切换．在根据预置定时切换密钥信息中，是否进行切换，切换周期或多条密钥信息的切换顺序也可用作提高加密等级、加密难易度或解密难度的密钥．

下面说明电路 13 至 18 的结构和加密的详例．

首先，如图 2 所示，扇区形成电路 13 被设计用于交错偶奇字节．这就是指，如图 2 所示，图 1 的接口电路 12 的输出数据被送至有二个输出端的转换开关 31．该开关的一输出端通过偶/奇交错器 33 被送至扇区形成电路 34，该开关的另一输出端直接送至扇区形成电路 34．扇区形成电路 34 以 2048 字节为单位采集输入数据以形成一个扇区．扇区形成电路 13 的转换开关 32 的转换操作受控于作为密钥来操作的一位控制信号．偶/奇交错器 33 将图 3A 所示的具有偶字节 36a 和奇字节 36b 交替排列的输入数据的一个扇区分配为如图 3 所示的偶字节数据段 37a 和奇字节数据段 37b，并输出这些数据段．而且，扇区内特定的数据段 39 可通过密钥信息来指定，并且只有在特定数据段 39 中的数据才可以分配在偶字节数据段 39a 和奇字节数据段 39b 中．在这种情况下，指定数据段 39 的方式可以被设计为从进一步增加密钥信息的可选种数以提高加密等级的多种方法中选择．加扰电路 14 使用被称作并行块同步类型的加扰器，所述加扰器采用一种如图 4 所示的 15 位移位寄存器．加到加扰器的数据输入端 35 的是从扇区形成电路 13 以最低有效位(LSB)首先在时间

上到来的次序，即被称作 LSB 最先的次序提供的数据．用于加扰的 15 位移位寄存器 14a 与根据生成多项式 $x^{15} + x + 1$ 提供反馈的异或(ExOR)电路 14b 相联系．因此，图 5 中所示的预置值或初始值被设置到 15 位移位寄存器 14a 上．同时，图 5 所示的预置值的选择号可在扇区的基础上根据，例如，扇区地址的低 4 位的值进行切换．移位寄存器 14a 的输出数据和在端子 35 的输入数据被异或电路 14c 异或以便在端子 14d 输出并送至图 1 中的首标附加电路 15．

根据密钥信息例如预置的识别号数可以改变所述的生成多项式和预置值(初始值)．即，可用图 6 所示的结构来改变生成多项式．在图 6 中，将移位寄存器 14a 的 15 位中的各位输出送至切换开关 14f 的固定端上，所述切换开关 14f 受控于控制端 14g 的例如 4 位控制数据．切换开关 14f 的输出被送至异或电路 14b．通过改变控制端 14g 的控制数据，就有可能改变生成多项式 $x^{15} + x^n + 1$ 中 n 的值．对于改变预置值而言，利用 16 字节识别信息中的每一字节值的算术运算，可以处理图 5 中预置值表的预置值．可以列举的识别信息有：媒体本身的识别信息，生产商识别信息，销售商识别信息，记录设备或编码器本身的识别信息，媒体生产设备本身的识别信息，地区信息或从外部提供的识别信息．上述信息可以相互组合或与其它信息组合使用．改变生成多项式的结构并不限于图 6 所示的结构，抽头的数目或移位寄存器的级数都可按需要改变．

下面详细说明首标附加电路 15．

图 7 表示扇区格式的一个具体的例子．每一个扇区由一个 2048 字节的用户数据区域 41 和附加在其上的 4 个字节的同步区域 42、16 字节的首标区域 43 及 4 字节的检错码(EDC)44 所组成．检错代码区域 44 的检错码由为用户数据区 41 和首标区 43 生成的 32 位 CRC 代码所组成．首标附加电路 15 中的加密可以在被称作数据同步、首标地址或 CRC 的同步信号上进行．

作为对扇区同步信号或数据同步加密的一个例子，如果分配给四字节同步区域 42 各字节的字节模式由图 8 中的 A、B、C、D 表示，则这些四字节内容可使用 2 位密钥信息来按字节进行移位或循环．这就是说，通过用 0、1、2 或 3 的 2 位密钥分别切换到 ABCD、BCDA、CDAB 或 DABC，如果和密钥数据不重合，则不能实现扇区同步，也即不能实现正常的重现．字节模式 A 到 D 可使用如 ISO 646 中的字符代码．

如图 9 所示，在首标区域 43 中形成有：用于被称为冗余循环代码 CRC 45 的各层，用于允许/禁止拷贝或管理拷贝生成的拷贝信息，表明多层盘的一个特定层的层 47，地址 48 和备用 49．加密可通过对地址 48 的 32 位进行位加扰，在这里是进行重排位序的方式来完成．如果使用 $x^{16} + x^{15} + x^2 + 1$ 作为 CRC 45 的生成多项式，也可改变响应于密钥的 x^{15} 至 x 的 15 个位取代第二项 x^{15} 和第三项 x^2 来进行加密．也可以通过算术操作处理 CRC 45 的 16 个位和处理密钥信息来进行加密．

可以列举的识别信息有：媒体本身的识别信息，生产商识别信息，销售商识别信息，记录设备、编码器或媒体生产设备本身的识别信息，地区信息或从外部提供的识别信息．上述信息可以相互组合或与其它信息组合使用．

图 10 和图 11 表明了纠错编码电路 16 的一个特定实施例．

在图 10 和图 11 中，图 1 中首标附加电路 15 所输出的数据通过输入端 51 送至 C1 编码器 52．在本特定实施例中，纠错和编码的每个帧由多达 148 字节或 148 符号的数据组成．输入端 51 的数字数据每次采集 148 个字节，并被送至作为第一编码单元的 C1 编码器 52．在 C1 编码器 52 中，附加一 8 字节的校验码，所得数据经过用于交错的延迟电路 53 送至作为第二编码单元的 C2 编码器 54．所述 C2 编码单元 54 附加于一个 14 字节的 Q 校验码的数据上，该 Q 校验码经延迟电路 55 反馈至 C1 编码器 52．包含 P 和 Q 校验码的 170 个字节从 C1 编码器 52 取出并经由延迟电路 56 和带有倒相器的重排电路 57 输出到输出端 58 以送至图 1 的调制电路 17．

对于上述纠错编码电路中的加密而言，需要考虑响应加密密钥信息而选择是否将倒相器插入到重排电路 57 中倒相部分 57a 的每个字节中．即，虽然 22 字节的 P 和 Q 校验码被所述基本结构中重排电路 57 的倒相部分 57a 的倒相器所倒相，这些倒相器中的某一些可省去不用或若干倒相器可被插入到 C1 数据中用于倒转输出的极性．

当执行所述数据转换时，不可能纠错的概率根据与所述基本结构的差别程度而变化，即，如果这种差别小，则最终被重现的输出数据出现差错的概率只有微小的增加，而如果差别很多，从整体上看纠错就变得很困难，因此重现几乎是不可能的．例如在 C1 编码器的情况下，作为表示纠错能力的指标的距离是 9，因此最大达到 4 个字节的检错和纠错是可能的，如果存在一个删除点，最大达到 8 个字节的纠错是可能的．因此，如果存在 5 个或更多

个差别，就总是不可能通过 C1 代码进行纠正．如果存在 4 个偏差，则出现脆弱的纠正状态，在至少再有一个差错时纠正就变为不可能．当差别从 3 到 2 到 1 递减时，可实行的纠错概率按上述顺序增大．如果利用这一点就一定能形成重现的状态，在这种状态下如果提供音频或视频的软件，重现在一定程度上是可能的，但不是完美无缺的，并且有时会发生紊乱．可以利用这一点来只让用户知道所述软件的概要．

在这种情况下，可使用把倒相器改变的位置规定在例如两处的方法，根据密钥信息随机地选择改变的位置并且限定改变位置的最小数字为两处的方法，或使用包含上述两种方法的组合的方法．

倒相器插入的或改变的位置并不限于图 10 和 11 所示的重排电路 57 中的位置， C1 编码器上游或下游的任何的位置或它们的各种组合都可以使用．在有多个位置的情况下，可以使用不同的密钥．对于数据转换而言，可使用位的相加或相似的逻辑运算来代替倒相器，可以根据用于加密的密钥信息来互换或替换数据．当然可单独或组合地使用各种加密技术如利用移位寄存器或各种功能处理来进行转换．

图 12 表示了纠错编码电路 16 的另外一个特定的实施例，其中一组异或(ExOR)电路 61 接入重排电路 57 中倒相器 57a 的下游，并且另一组异或电路 66 接入 C1 编码器 52 输入端的上游．

具体地说，所述异或电路组 61 对从 C1 编码器 52 输出和经过延迟电路 56 和重排电路 57 中的倒相器部分 57a 的 170 字节的数据进行异或操作的数据转换，即对信息数据 $C_{170n\cdot 169}$ ~ $C_{170n\cdot 22}$ 和校验数据 $P_{170n\cdot 21}$ ~ $P_{170n\cdot 14}$，$Q_{170n\cdot 13}$ ~ Q_{170n} 进行异或操作的数据转换，而异或电路组 66 则对 148 字节的输入数据 B_{148m} ~ $B_{148n\cdot 147}$ 进行异或操作的数据转换．在异或电路组 61、 66 中使用的异或电路对 1 个字节的或 8 位的输入数据和由 1 位控制数据确定的 8 位预置数据进行异或操作．这些 8 位异或电路(如果预置的 8 位数据等于零，则与倒相器电路相等)中的 170 个和 148 个分别用于异或电路组 61、 66 中．

在图 12 中， 170 位密钥信息被送至端子 62 并且通过一个被称作 D－锁存器的电路 63 路由到异或电路组 61 的 170 个异或电路中的每一个． D－锁存电路 63 响应于送至使能端 64 的 1 位加密控制信号而切换下列二者之一：从端子 62 直接发送 170 位密钥信息至异或电路组 61 和将全部的 170 位设置为“ 0 ”．所述异或电路组 61 的 170 个异或电路当中．从 D－锁存电路 63

提供“0”值的异或电路直接从重排电路57中的倒相器部分57a输出数据，而从D－锁存电路63提供“1”值的异或电路则把从重排电路57中的倒相器部分57a来的数据进行倒相然后输出．在所有值为0的情况下，直接从重排电路57中的倒相器部分57a输出数据．除了包括148个异或电路和带有148位的密钥信息之外，异或电路组66和异或电路组61的装置很相似，因此，输送到端子67的148位密钥信息经过D－锁存电路68被送至所述异或电路组中的每一个异或电路．D－锁存电路68通过使能端69的加密控制信号切换到148位密钥信息或全部零值．

在图12所示的电路中，异或电路组61对从C1编码器52输出并经过延迟电路56和重排电路57的倒相器部57a的170字节的数据进行异或操作的数据转换，即对信息数据$C_{170n\cdot169}$～$C_{170n\cdot22}$和校验数据$P_{170n\cdot21}$～$P_{170n\cdot14}$，$Q_{170n\cdot13}$～Q_{170n}进行异或操作的数据转换．另一方面，异或电路组61可根据148字节的密钥信息设计成对148字节的信息数据$C_{170n\cdot169}$～$C_{170n\cdot22}$而不对校验数据进行数据转换．

使用图12所示的电路，可实现同图10和11中所示电路相似的操作和效果．也可能使用异或电路61和66之一组或者使用两组异或电路之一组成两组的选择作为加密密钥．

可以列举的密钥信息有：媒体专用的识别信息，生产商识别信息、销售商识别信息、记录设备、编码器或媒体生产设备专用的识别信息，地区信息，或从外部提供的识别信息．上述信息可相互组合使用或与其它信息组合使用．

也可以使用与门、或门、与非门、或非门或倒相器电路来取代异或电路61和62作为上述的数据转换设备．除了利用1位的密钥信息或在8位基础上的密钥数据进行逻辑处理外，还可对8位信息数据进行逻辑处理．另一方面，与门、或门、异或门、与非门、或非门或倒相器电路可组合使用于与信息数据的1个字对应的8位中的各位．在这种情况下，148×8位的密钥数据被用于148字节的数据，即148×8位的数据．而且，如果组合地使用与门、或门、异或门、与非门、或非门或倒相器电路，这些组合本身也可作为密钥来使用．当然可使用各种加密技术，如利用移位寄存器或各种功能处理而进行的转换，使得它们也可以组合起来使用．

在第一实施例中说明了交叉交错型纠错码，但它也可应用于乘积码，以

后将对其作为本发明的第二实施例进行说明.

现在参照图 13 说明图 1 中调制电路 17 的加密. 在此图中, 从纠错编码电路 16 输出的数据每 8 位(1 个字节)送至端子 71, 而 8 位密钥信息则送至输入端子 72. 这些 8 位数据被送至作为逻辑处理电路一例的异或电路 73 用以执行异或操作. 异或电路 73 的 8 位输出被送至预置的调制系统的调制器, 如 8 - 16 转换电路 74, 以转换到 16 通道位. 由 8 - 16 转换电路 74 进行 8 - 16 转换的系统的一个实例被称为 EFM + 调制系统.

虽然使用 8 位密钥信息的加密在数据调制之前, 但是密钥信息的位数不局限于 8, 而用于 8 - 16 转换的转换表的输入 - 输出的相互关系可以根据密钥信息来改变. 当然对于密钥信息而言, 也可使用以上描述的记录媒体专用的识别信息.

下面说明同步附加电路 18.

同步附加电路 18 使用图 14 所示的 S0 至 S4 四种同步字来产生以 8 - 16 调制帧为单位的同步. 例如, 对作为 8 - 16 调制的一个帧的 85 个数据符号或 1360 通道位附加一个 32 通道位的同步字, 该帧的构成与 C1 或 C2 代码有关, 使 C1 代码串的领先帧的同步字不同于另一帧的同步字, 用以产生 S0 到 S3 四种同步字 S0 至 S3. 这些同步字 S0 至 S3, 根据直接在前面的字的 "0" 或 "1" 的状态, 即根据所谓的数字和或 dc 值, 各自具有 a 和 b 两种同步模式.

根据密钥信息 75 的两位, 使用图 15 所示的电路, 可以改变对 S0 到 S3 这四种同步字的选择以实现加密的目的. 这就是指, 表示 S0 到 S3 四个同步字的两位数据 76 的各位和表示 2 位密钥信息 75 的相应位用二个异或电路 77、78 来异或以产生新的同步字表示数据 79. 这就改变了上述帧结构中使用同步字的方式或上述帧结构中使用不同种类的同步字的情况(position), 以实现加密的目的.

也可能增加同步字种类的数量和根据加密的密钥确定从这些同步字中取出这四种同步字的方式. 上述的记录媒体专用的识别信息可作为这种密钥信息来使用.

图 16 表示作为记录媒体一例的盘状记录媒体 101, 如光盘. 所述盘状记录媒体 101 从内缘向外缘看具有一中心孔 102, 作为目录区域(TOC)或程序管理区域的导入区域 103, 用于记录程序数据的程序区域 104, 及程序结

尾区域或导出区域 105．在用于重现音频信号或视频信号的光盘中，音频或视频数据记录在所述程序区域中，音频或视频数据的时间信息由导入区域 103 管理.

写入与程序区域不同的区域中的识别信息，可作为密钥信息的一部分．具体地说，该识别信息可写入作为目录区域的导入区域 103 或导出区域 105．所述识别信息包括：记录媒体专用的识别信息例如产品号码，生产商识别信息，销售商识别信息，记录装置或编码器专用的识别信息或生产记录媒体的设备如切割机或冲压机专用的识别信息，经过上述 6 个电路 13 至 18 中至少一个最好是两个电路中的加密而得到的信号被记录在作为数据记录区域的程序区域 104 中．为了重现，可使用上述识别信息用于解密．所述识别信息也可用物理或化学方法写入导入区域 103 中，并且在重现过程中被读出以作为解码用的密钥信息使用.

下面将参照图 17 说明本发明的数据重现方法和数据重现装置的优选实施例.

在图 17 中，作为一种记录媒体例子的盘状记录媒体 101 随主轴电机 108 转动，以便被重现头装置 109，如光学拾取头，读取记录内容.

经重现头装置 109 读取的数字信号被送至目录解码编器 111 和放大器 112 中．识别信息从目录解码器 111 中读出以至少作为用于解密的密钥信息的一部分．所述识别信息包括：记录媒体专用的识别信息如产品号码，生产商识别信息，销售商识别信息，记录装置或编码器专用的识别信息，或生产记录媒体的设备如切割机或冲压机专用的识别信息．重现装置专用的识别信息或外来的识别信息可以从所述重现装置中的 CPU 122 输出以便至少作为密钥信息的一部分．外来的识别信息包括经通信网络或传输路径接收的识别信息和从 IC 卡、ROM 卡，磁卡或光卡读取的识别信息.

从重现头装置 109 输出的数字信号经放大器 112 和锁相环(PLL)电路 113 被送至同步分离电路 114，所述同步分离电路用于分离由图 1 中同步附加电路 18 附加的同步信号．从同步分离电路 114 输出的数字信号被送至解调电路 115，所述解调电路执行与图 1 中调制电路 17 相反的操作．具体地说，此操作将 16 通道位的数据转换为 8 位的数据．从解调电路 115 输出的数字数据被送至纠错解码电路 116，所述纠错解码电路执行与图 1 中纠错编码电路 16 相反的操作．已解码数据被一个扇区分解电路 117 分解为许多扇区，并且每

个扇区前端的首标被首标分离电路 118 所分离. 扇区分解电路 117 和首标分离电路 118 分别对应于图 1 中的扇区形成电路 13 和首标附加电路 15. 解扰电路 119 执行与图 1 中加扰电路 14 加扰相反的解扰操作以使重现的数据经接口电路 120 在输出端 121 输出.

应该注意的是, 加密至少已在记录过程中的下列电路之一中进行: 扇区形成电路 13, 加扰电路 14, 首标附加电路 15, 纠错编码电路 16, 调制电路 17 和同步附加电路 18. 因此, 需要在与所述加密电路相对应的重现侧电路 114 至 119 中执行解密操作. 即, 如果在图 1 中的扇区形成电路 13 中进行加密, 则需要在扇区分解电路 117 中使用用于加密的密钥信息进行解密. 相似地, 解扰电路 119、首标分离电路 118, 纠错解码电路 116、解调电路 115、和同步分离电路 114 中的解密需要分别与图 1 中的加扰电路 14, 首标附加电路 15, 纠错编码电路 16、调制电路 17 和同步附加电路 18 的加密相联系.

同步分离电路 114 通过在帧结构中检测多个, 如 4 个, 不同种类的同步字的使用方式或各种同步字的使用情况来进行解密, 如参照图 14 和 15 所说明的, 所述使用方式和使用情况已根据用于加密的密钥信息有了改变.

在由解调电路 115 进行解密操作中, 从同步分离电路 114 送至 16 到 8 转换电路 131 以便从 16 通道位转换的 8 位数据被送至与图 13 中的异或电路 32 相对应的异或电路 132, 以便与从端子 133 输入的 8 位密钥信息相异或, 从而恢复相应于图 13 中送至输入端 71 的 8 字节数据, 如图 18 所示. 被恢复的数据被送至纠错解码电路 116.

纠错解码电路 116 通过图 19 和 20 的结构执行与图 10 和 11 所示的纠错编码电路相反的操作.

参照图 19 和 20, 从解调电路 115 输出的已解调数据以 170 个字节或 170 个符号为单位, 经带有倒相器 142a 的重排电路 142 和延迟电路 143, 被送至作为第一解码器的 C1 解码器 144. 在送至 C1 解码器 144 的 170 字节数据中, 有 22 字节的数据是 P 校验数据和 Q 校验数据. C1 解码器 144 利用这些校验数据进行解码. C1 校验数据经延迟电路 145 将 170 字节的数据送至作为第二解码器的 C2 解码器 146, 在所述 C2 解码器 146 中, 使用这些校验数据进行纠错和解码. C2 解码器 146 的输出数据被送至图 19 中的延迟 C1 解码电路 140. 这个电路与延迟电路 143 和 C1 解码器 144 相似, 并重复地执行与延迟电路 143 和 C1 解码器 144 相似的操作, 以进行纠错和解码. 图 20 所述

的实施例中，延迟 C1 解码电路 140 表示为延迟电路 147 和作为第三解码器的 C3 解码器。延迟电路 147 和 C3 解码器 148 或延迟— C1 解码电路 140 执行最终的纠错和解码以便使不具有校验码的 148 字节数据在输出端 149 输出。所述的 148 字节的数据与输入图 11 的 C1 编码器 52 的 148 字节的数据相对应。

如果加密已在图 10 和 11 中纠错编码电路的重排电路 57 的倒相器部分 57a 中进行，就需要在图 19 和 20 中纠错和解码电路重排电路 142 的倒相器部分 142a 进行相应的解密。当然需要执行与参照图 10 和 11 所说明的各种加密相反的解密操作。

图 21 表示了与图 12 中纠错编码电路的结构相对应的纠错解码电路。

参照图 21，异或电路组 151 被接入到重排电路 142 的倒相器部分 142a 的输入侧和延迟电路 143 的输入侧，所述异或电路组 151 相应于接入到图 12 中重排电路 57 的倒相器部分 57a 输出侧的异或电路组 61，而异或电路组 156 被接入到 C3 解码器 148 的输出侧，相应于接入到图 12 中 C1 编码器 52 的输入侧的异或电路组 66。

所述异或电路组 151 、 156 的结构用于对图 12 中异或电路组 61 、 66 执行的数据斩进行数据转换的解译。这两个异或电路组中异或电路组 151 由 170 个 8 位异或电路所组成，而异或电路组 156 由 148 个 8 位异或电路所组成。如果已由图 12 中纠错编码电路记录侧的异或电路 61 对除了校验数据以外的 148 字节信息数据进行了响应于密钥信息的数据转换，则异或电路组 151 自然地由 148 个 8 位异或电路所构成。

相应于输送至图 12 的端子 62 的密钥信息的 170 位密钥信息被送至图 21 的端子 152。经由 D 锁存电路 153 将密钥信息输送至异或电路组 151 中 170 个异或电路中的每一个。所述 D 锁存电路 153 响应于输送到使能端 154 的 1 位加密控制信号，在下述两种操作间进行转换：从端子 152 直接输出 170 字节的密钥信息到异或电路组 151 和将 170 个字节全部设置为“ 0 ”(全零)。另一方面，异或电路组 156 与异或电路组 151 相似，但是异或电路组 156 具有 148 个异或电路和具有与输送至图 12 的端子 12 的密钥信息相同的 148 位密钥信息。输送到端子 157 的所述 148 位的密钥信息经过 D 锁存电路 158 送至 148 个异或电路中的每一个电路。所述 D 锁存电路 158 又响应于从使能端 159 输入的加密控制信号在 148 位的密钥信息和全零之间进行转换。

利用所述的异或电路或所述纠错电路的倒相器，就可能实现简单但是有效的加密．而且，通过控制倒相器的数量，可以根据保密等级的要求来解决所述加密等级中通常不可重现的数据或在加重的差错状态下成为不可重现的数据．即，通过控制倒相器或异或电路的数目，可以进行这样的控制，对应于更好的和更坏的差错状态，使重现分别变得可能和不可能．而且，不能通过纠错本身恢复的可重现状态也能产生出来．对于加密密钥而言，在每个加密地点位的数目甚至可达到 100 或 100 个以上，上述的实施例就是如此．由此可使用大量的密钥的位数进行加密以提高数据安全性．而且，通过在 LSI 或 IC 芯片硬件中实现纠错编码电路和纠错解码电路，可使一般的用户很难进入记录媒体，因此再次提高了数据的安全性．

扇区分解电路 117 进行被称为解除交错的操作，即，如果按参照图 2 和 3 所作的说明，在记录过程中已经由扇区形成电路 13 通过交错奇或偶字节进行了加密，则上述的解除交错操作是与这种奇或偶交错相反的操作．

如果按参照图 7 至 9 所作的说明，已经使用首标附加电路 15 在记录过程中进行了加密，即进行了表示扇区同步、地址变化或 CRC 变化的数据同步字节模式置换，则首标分离电路 118 进行相对应的解密．

图 22 表示解扰电路 119 的说明性实施例．从图 17 首标分离电路 118 输出的数字数据被送至端子 161．从端子 161 输出的数字数据被图 4 中的加扰器解扰，以便在输出端 164 输出．根据从认可(authorization)机构 171 输出的加密密钥信息，通过改变多项式 165 和预置值或初始值 166(见参照图 4 对加扰器所作的说明)来进行解扰．根据首标信息 167 中复制信息 46 的内容、记录媒体或重现装置专用的识别信息 172、生产商或销售商的通用识别信息 173 或由外部提供的外部识别信息 174，认可机构 171 产生加密密钥信息以根据该密钥信息来控制生成多项式 165 或预置值 166．

如前所述，有关需要在电路 114 至 119 的哪一个电路中解密的信息成为用于加密的密钥信息．而且，加密密钥信息可在预置的周期内，如每个扇区内，进行切换．通过把是否进行切换、或把切换周期作为密钥使用，提高了加密的难易程度．

通过将生产商识别信息、销售商识别信息或装置识别信息与复制防止信息或收费信息相组合，如上所述各别地设置这些信息以对数据加密和记录被加密的数据，能够在物理格式的层次上实现防止复制、非法翻版或非法使用．

另外，有关数据安全功能的信息、拷贝允许/禁止信息或收费/免费信息在记录媒体上或在记录/重现系统的物理格式中得到了实现。

这就是说，通过在记录媒体上预先记录安全/收费信息和将这一信息与使用记录媒体的可记录/不可记录的信息的数据加密相组合，就可用简化的结构来实现防止拷贝和防止非法使用。通过在物理格式中的隐藏包容(latent incorporation)，就可使解码变得困难。由于结构仍停留在加密状态，因此所述结构是安全的，可以防止转贮拷贝。所述结构可在扇区、文件、区段或层的基础上变化。而且，可以通过通讯、IC 卡、或用遥控器来进行密钥控制。也可听任滞后(hysteresis)来防止剽窃。

下面说明本发明的第二实施例。

第二实施例是上述第一实施例的部分改型。其整体结构如图 1 所示。下面只说明图 1 中的结构的电路 13 至 18 改型的部分。

图 1 的扇区形成电路 13 可按照上述第一实施例那样配置。但是，加扰电路 14 则按图 23 所示的那样来配置。

如图 23 所示在加扰电路 14 中，从图 1 的扇区形成电路 13 输出的数据以最低有效的位先输出的顺序，即 LSB 第一的顺序，输送至数据输入端 35。构造一个用于加扰的 15 位移位寄存器 14a 以便通过使用异或(ExOR)电路 14b 来提供生成多项式 $x^{15} + x^4 + 1$ 的反馈，而图 24 所示的预置值或初始值被设置在 15 位移位寄存器 14a 中。对图 24 所示的预置值的选择号进行选择，这样便可在扇区的基础上结合例如扇区地址的低 4 位的值对预置值进行切换。移位寄存器 14a 的输出数据与端子 35 的输入数据被异或电路 14c 所异或，其中输出在输出端 14d 输出以送至图 1 的首标附加电路 15。

预置值(初始值)可根据密钥信息如预置的识别号数而改变。即，可使用 16 字节识别信息的各个字节的值对图 24 预置值表中的 16 字节识别信息的预置值进行逻辑处理。在这种情况下，识别信息可包括如下识别信息之一或它们的组合：记录媒体专用的产品号码，生产商识别信息、销售商识别信息，记录装置或编码器专用的识别信息或生产记录媒体的设备专用的识别信息、地区信息、从外部提供的识别信息。上述各种信息也可与其它信息组合使用。逻辑处理包括异或(ExOR)，逻辑积(AND)、逻辑和(OR)或移位。

用于第二实施例的扇区格式可以如图 25 那样来构造。

在图 25 中，每个扇区由各为 172 个字节的 12 行，总共 2064 个字节所

组成，其中的2048个字节表示主要数据．一个4字节的识别数据(ID)排列在12行中第1行的最前面位置，接下来的顺序是2字节的ID检错码(IED)，6字节的保留数据(RSV)．在最后一行的最后位置上排列4字节的检错码(EDC).

如图26所示，识别数据(ID)的4个字节由扇区信息形成的第一字节(631到624位)和扇区号形成的剩下三个字节(623到60位)所组成．所述扇区信息由1位的扇区格式类型，1位的跟踪方法，1位的反射率，1位的备用信息，2位的区域类型和2位的层号所组成．

图1的首标附加电路15执行倒换(transposition)功能，即，根据密钥信息对扇区格式中识别数据(ID)的24位扇区数字在位的基础上进行加扰，以执行加密．另外，为了执行加密，可根据密钥信息对2字节的ID检错码(IED)的生成多项式或4字节的检错码(EDC)的生成多项式进行修改，或用密钥信息对其进行逻辑处理．

图1中的纠错编码电路16可以如图27那样来构造．对于编码，使用如图28所示的乘积码或块码．

参照图27，从图1所示的首标附加电路15输出的数据被送至输入端210．输入数据被送至作为第一编码单位的P0编码器211．输入至P0编码器211的输入数据有172字节乘192行或B_{00}到$B_{191,171}$．如图28所示，P0编码器211将作为16字节里德－索洛蒙码(RS code)的RS(208, 192, 17)的RS外码附加于172列的192字节的每一列．P0编码器211的输出数据经上述用于加密的数据转换电路212送至交错电路213，以形成输入到PI编码器214的经交错后的数据．PI编码器214将RS(182, 172, 11)(RS代码)的RS内码(PI)附加于172字节乘208行的172个字节的每一行．因此，PI编码器214输出182字节乘208行的数据．这些输出数据经上述用于加密的数据转换电路215被输出到输出端216．

由于P0编码器211将16字节的P0校验码附加于192字节的输入数据以使每一列输出208字节的数据，因此数据转换电路212对16字节的校验码或全部208字节的数据进行上述的数据转换以进行加密．这种数据转换可响应于经端子218输入的密钥信息来进行．由于PI编码器214将10字节的PI校验码附加于每行的172字节数据，以输出182字节的数据，因此数据转换电路215可通过对该10字节校验数据或全部182字节数据的数据转换来进行

加密. 这种数据转换如前所述可响应于经端子 219 输入的密钥信息来进行.

上述的数据转换可通过在预置位置上安排一个倒相器, 通过根据密钥信息而利用异或电路组有选择地对数据倒相, 或通过使用与门、或门、或者与非门电路来进行. 除了利用 1 位密钥信息数据或密钥数据对 8 位信息数据进行逻辑处理外, 也可利用 8 位的密钥信息数据对 8 位信息数据进行逻辑处理, 或者, 可以组合使用与门、或门、异或门、与非门、或非门或倒相器电路来使每个 8 位组成信息数据的一个字. 当然, 各种加密技术, 如利用移位寄存器或利用功能处理的转换, 可单独或组合使用. 如果与门、或门、异或门、与非门、或非门或倒相器电路组合使用, 可将组合本身作为密钥使用. 而且, 除了逻辑处理之外, 改变数据位置的倒换或取代数据值的替换也可以作为数据转换来使用. 当然, 各种加密技术, 如利用移位寄存器或利用功能处理的转换, 可单独或组合使用.

从纠错编码电路获得的 182 × 208 个字节的数据相对于行被交错并且被分成 13 行 1 组共 16 组, 其中每一组与一个记录扇区相联系. 由 182 个字节乘 13 行共 2366 个字节组成的每个扇区被调制并且每一行附加两个同步代码 SY, 如图 29 所示. 对于调制而言, 使用如上述第一实施例中的 8 到 16 位转换. 每一行被分成两个同步帧, 其中的每个同步帧由一个 32 通道位同步代码 SY 和一个 1456 通道位的数据段所组成. 图 29 表示了经调制获得的一个扇区的数据结构和附加的同步数据. 图 29 中每一扇区的 38688 通道位与调制之前的 2418 字节相对应.

图 29 中的已调制输出信号使用 SY0 到 SY7 八种同步代码. 相应于上述的 8 - 16 转换状态, 这些同步代码 SY0 到 SY7 分别表示图 30(a)的 8 - 16 转换状态 1, 2 的同步模式和图 30(b)的 8 - 16 转换状态 3, 4 的同步模式.

可响应于用于加密的 3 位密钥信息来改变八种同步代码 SY0 到 SY7 的选择. 即, 表示八种同步代码 SY0 到 SY7 的 3 位数据 221 的各位和 3 位密钥信息 222 被 3 个异或电路 223, 224, 225 异或以产生表示数据 226 的新的同步代码. 这就改变了在上述帧结构中使用同步代码的方式或上述帧结构中使用各种同步代码的情况以进行加密. 当然, 根据密钥信息, 可通过移位寄存器或通过功能转换对 3 位数据进行倒换、替换或转换.

作为与本发明第二实施例记录侧结构相对应的重现侧的基本结构与图 17 所示的结构相似, 它执行随第二实施例的改型部分而改型的相反的操作.

例如，作为与图 27 中的纠错编码相对应的所述相反的操作可利用图 32 中的纠错解码电路来实现。

在图 32 中，图 28 的 182 × 208 个字节的乘积码的数据相应于图 27 中输出端 216 的输出，即图 17 中解调电路 115 的输出信号，该乘积码数据被输入至输入端 230。从输入端 230 输出的数据被送至数据反转换电路 231，在这里执行与图 27 中数据转换电路 215 相反的操作。数据反转换电路 231 输出的数据被输入至 PI(内码)解码器 232，执行作为与图 27 中 PI 编码器 214 相反的操作，在这里将进行解码，即，使用 PI 代码进行纠错，以产生图 28 所示的 172 × 208 个字节的数据。PI 解码器 232 的输出数据被与数据转换电路 213 所执行的操作相反的操作来处理，继而被输送至 P0(外码)解码器 235。P0 解码器 235 执行与图 27 中 P0 编码器 211 相反的操作，即，使用 P0 代码进行纠错，以便在输出端 236 取出 172 × 182 个字节的原始数据。如果图 27 的数据转换电路 212, 215 使用密钥信息进行数据转换，则输入到端子 218, 219 的密钥信息可被输入至图 32 的数据反转换电路 234, 231 的端子 239, 238，以便根据密钥信息进行数据反转换。

本发明的上述第二实施例的良好效果与上述第一实施例的相似。

在本发明的数据记录方法的上述实施例中，至少在下述步骤之一加密处理输入数据：以预置的数据量划分输入数字数据的扇区形成步骤，附加首标的首标附加步骤，根据预置的调制系统进行调制的调制步骤，附加同步模式的同步附加步骤。然后输出所得到的加密数据，使得已进行加密的特定的步骤也成为加密的密钥，因此提高了加密的难易程度。用于消除相同模式的对数据实施随机化的加扰步骤也可包括在各加密步骤中间。还有一个优点就是通过简单地部分改变预先存在的结构可以很容易地实现加密。使用所述的数据记录装置，记录媒体，数据重现方法或数据重现装置能够实现上述效果。

由于数据转换是至少对在纠错编码过程中处理的数据的一部分进行的，因此根据加密的密钥信息可以实现两种需要的等级的加密，即利用纠错编码来一定程度地恢复数据是可能的等级和恢复数据是不可能的等级。这就有可能进行控制，使得对于可接受的差错状态重现是可能的或者对于不可接受的差错状态重现是不可能的，由此使得根据数据的使用或安全等级来进行调节成为可能。

另外，在纠错中使用较大量的密钥位数进行加密成为可能，并且加密在

一个巨大的黑盒中如纠错编码或解码的 IC 或 LSI 中进行，因此使一般的用户很难解密，于是大大提高了数据的安全性。

此外，使用了预置的密钥信息对数据加密，且用于加密的密钥信息至少有一部分被写入与数据记录媒体上的数据记录区域不同的区域，以便使这部分密钥信息在重现过程中被读出并用于解密。所述密钥信息并不完整地存在于记录媒体的数据记录区域中的信息中，因此提高了解密的难度。

再有，在主要目的是对数据实施随机化以消除数据串中相同同步模式的加扰操作过程中，响应于加密密钥，生成多项式或初始值至少其中之一被改变，因此可直接使用预先存在的加扰来进行加密以便用简化的结构实现加密。

通过上述的数据加密，可采用一个简化的结构实现防止拷贝或非法使用，也可很容易地将其应用于安全或收费系统中。

本发明并不限于上述的实施例，例如，除了上述的倒相器或异电路之外，使用位的相加或各种逻辑操作，也可实现数据转换。还可以单独或组合地使用各种加密技术，如响应于加密密钥信息而利用移位寄存器或各种功能处理的数据替换、替换或倒换。也可以作出各种其它的修改而不离开本发明的要旨。

说 明 书 附 图

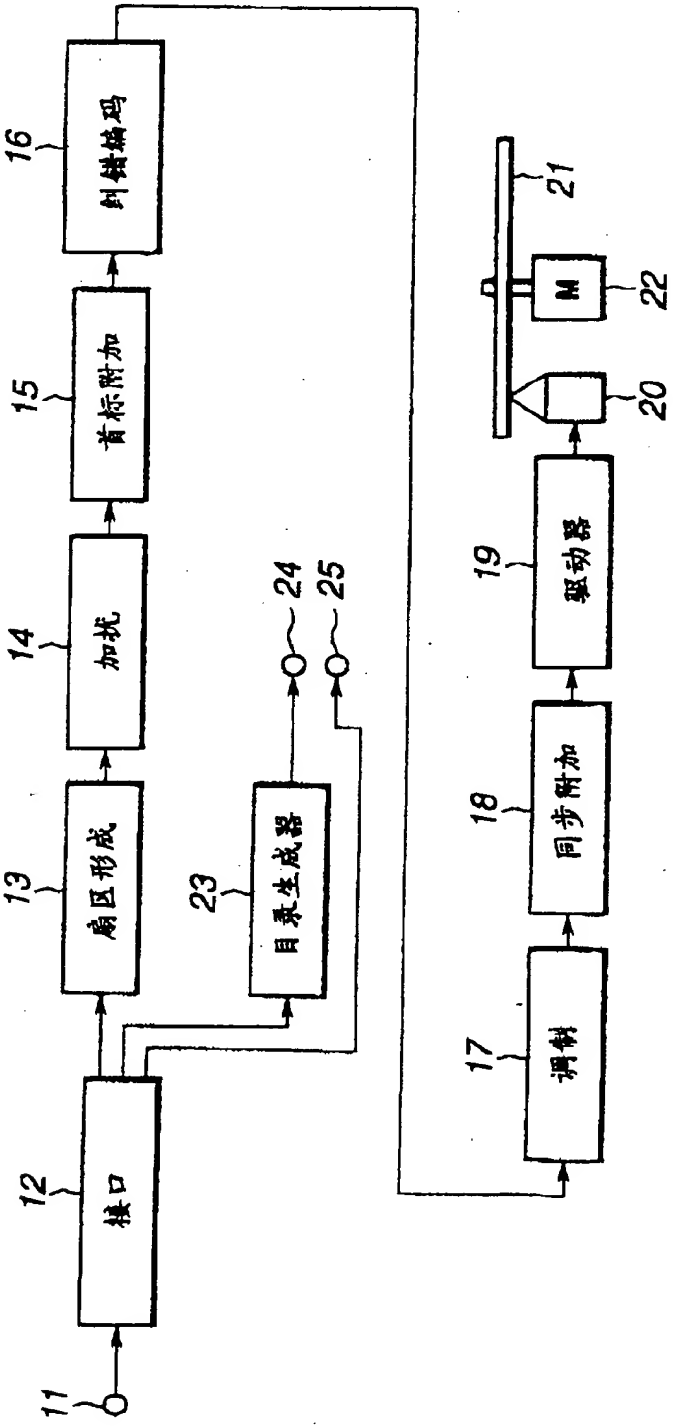

11
12
接口
13
扇区形成
14
加扰
15
首标附加
16
纠错编码
17
调制
18
同步附加
19
驱动器
20
21
M
22
23
目录生成器
24
25

图 1

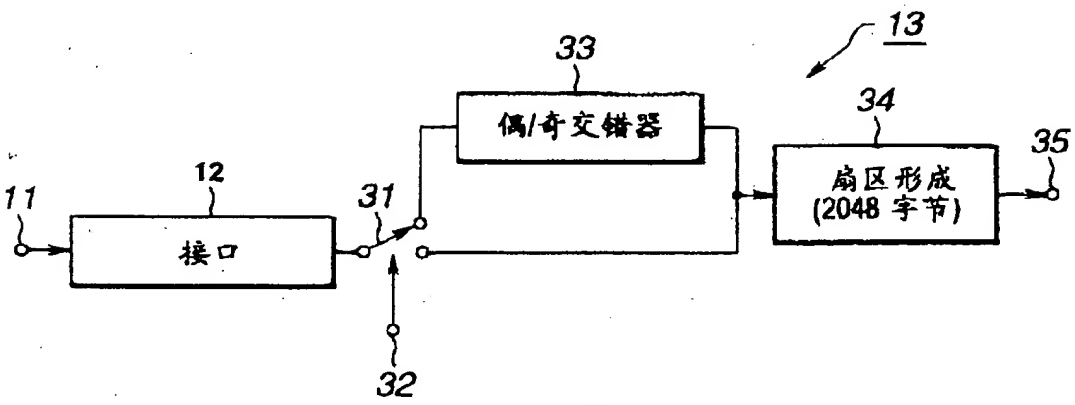

13
33
偶/奇交错器
34
35
扇区形成
(2048 字节)
12
11
31
接口
32

图 2

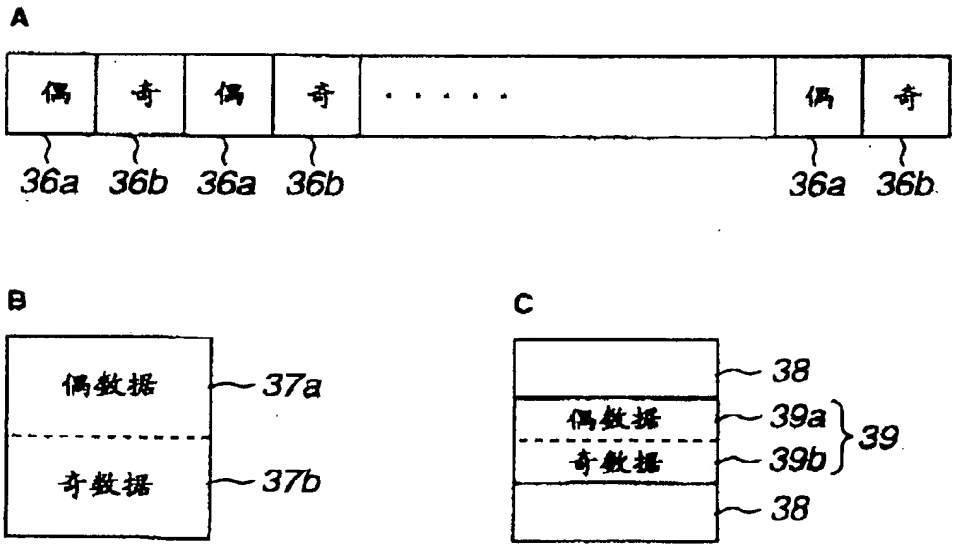

A
偶
奇
偶
奇
偶
奇
36a
36b
36a
36b
36a
36b
B
偶数据
37a
奇数据
37b
C
38
偶数据
39a
奇数据
39b
39
38

图 3

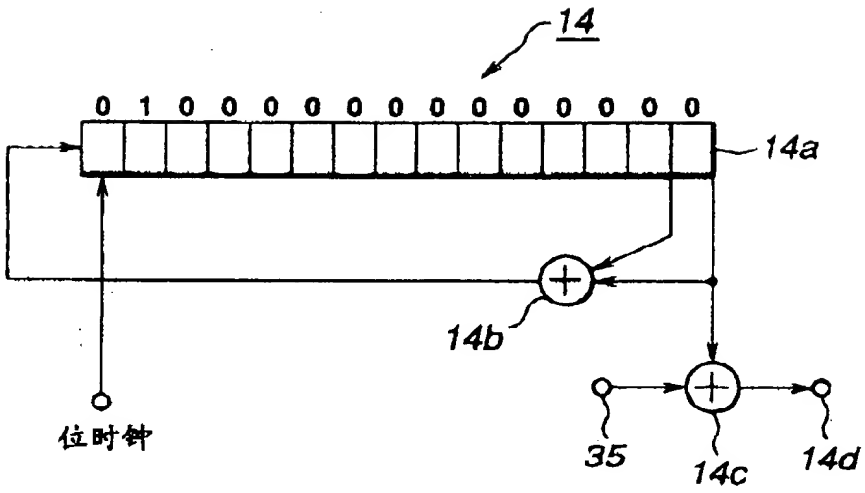


图 4

选择号	预置值	选择号	预置值
0	$0001	8	$4080
1	$4000	9	$2040
2	$2000	10	$1020
3	$1000	11	$0810
4	$0800	12	$0408
5	$0400	13	$0204
6	$0200	14	$0102
7	$0100	15	$4081

图 5

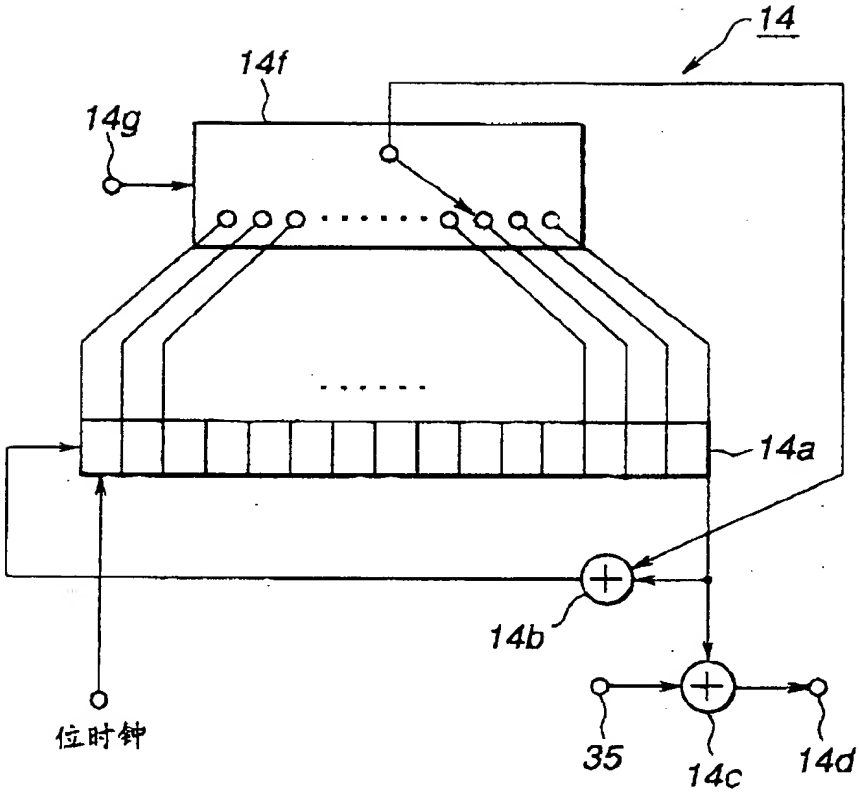


图 6

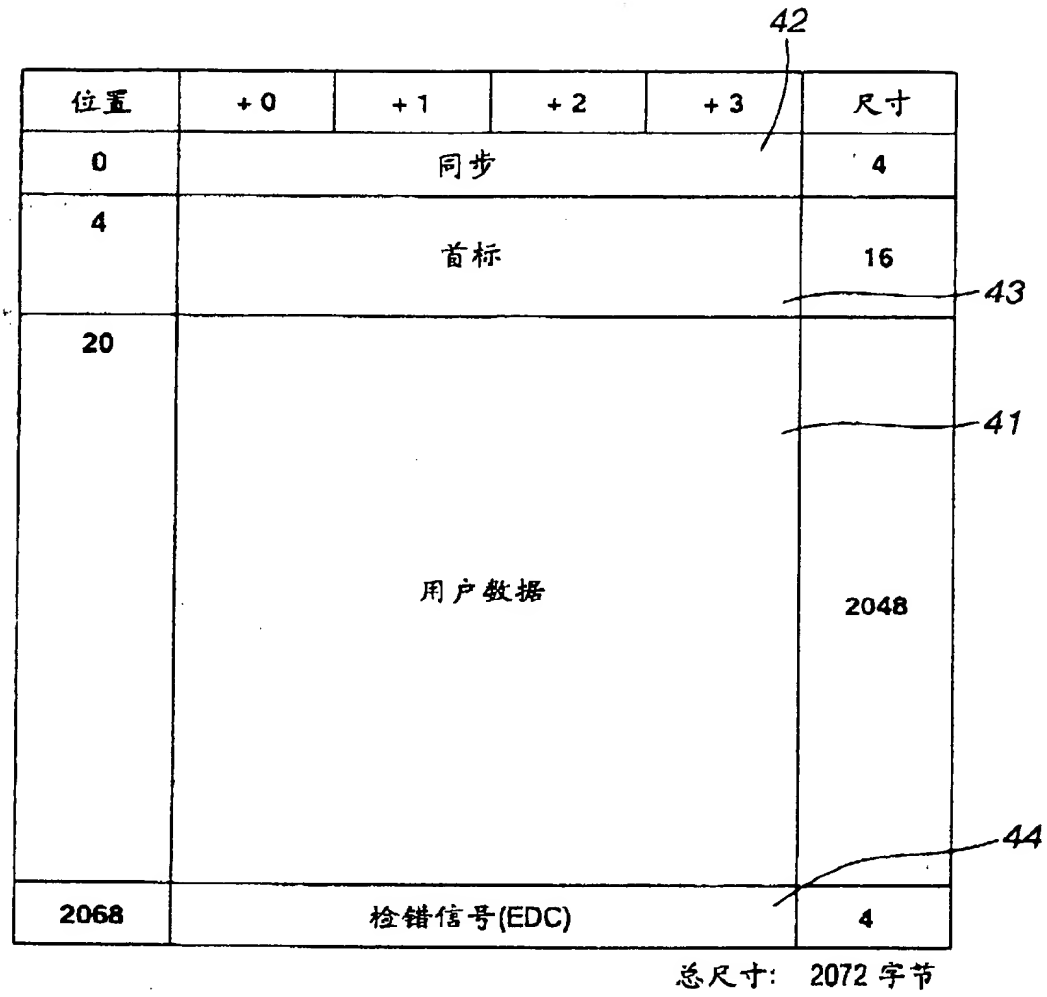

42
位置
+0
+1
+2
+3
尺寸
0
同步
4
4
首标
16
43
20
41
用户数据
2048
44
2068
检错信号(EDC)
4
总尺寸: 2072 字节

图 7

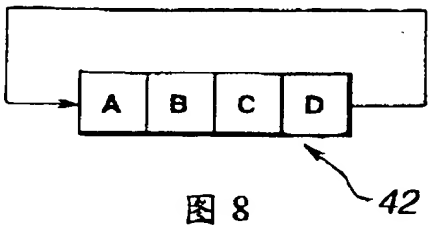

A
B
C
D
42

图 8

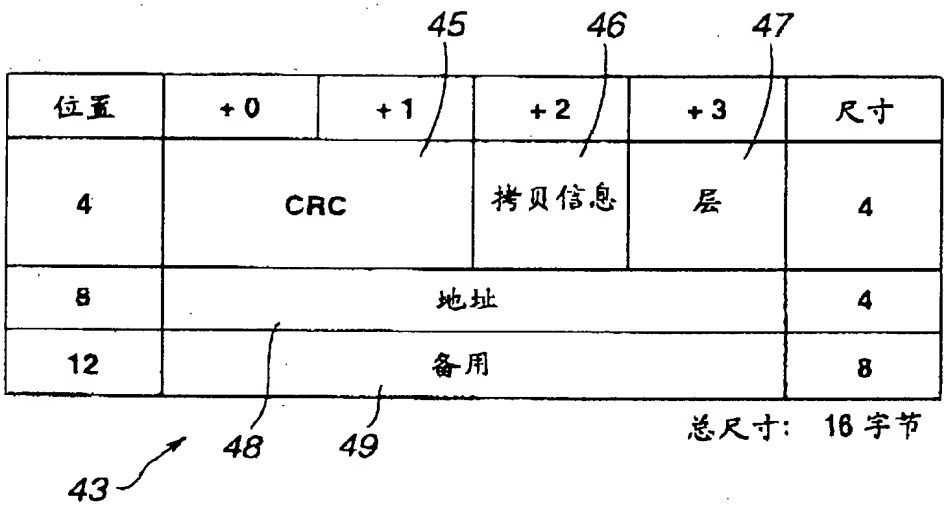


图 9

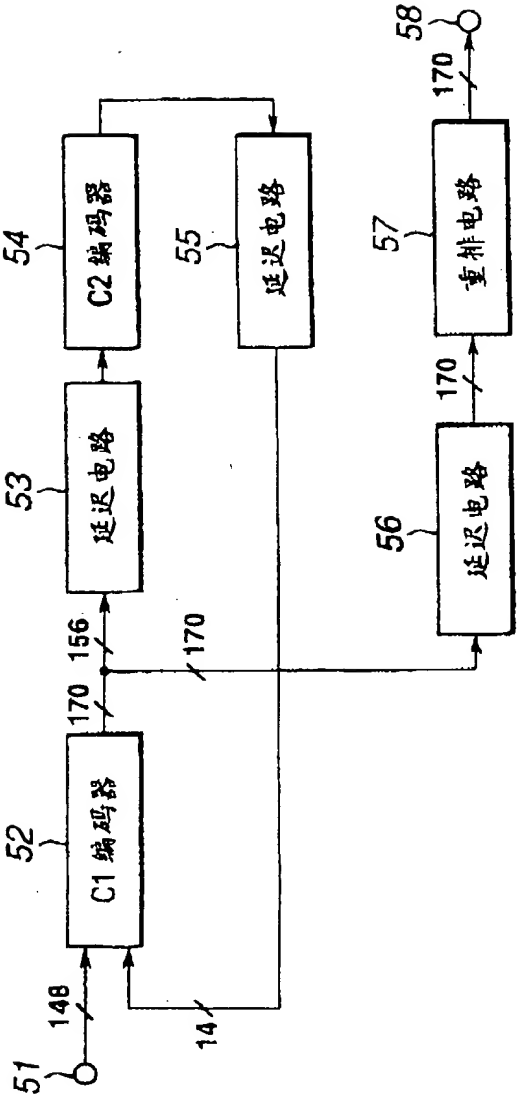

51
148
52
C1 编码器
14
54
C2 编码器
53
延迟电路
55
延迟电路
156
170
170
170
56
延迟电路
57
重排电路
170
58

图 10

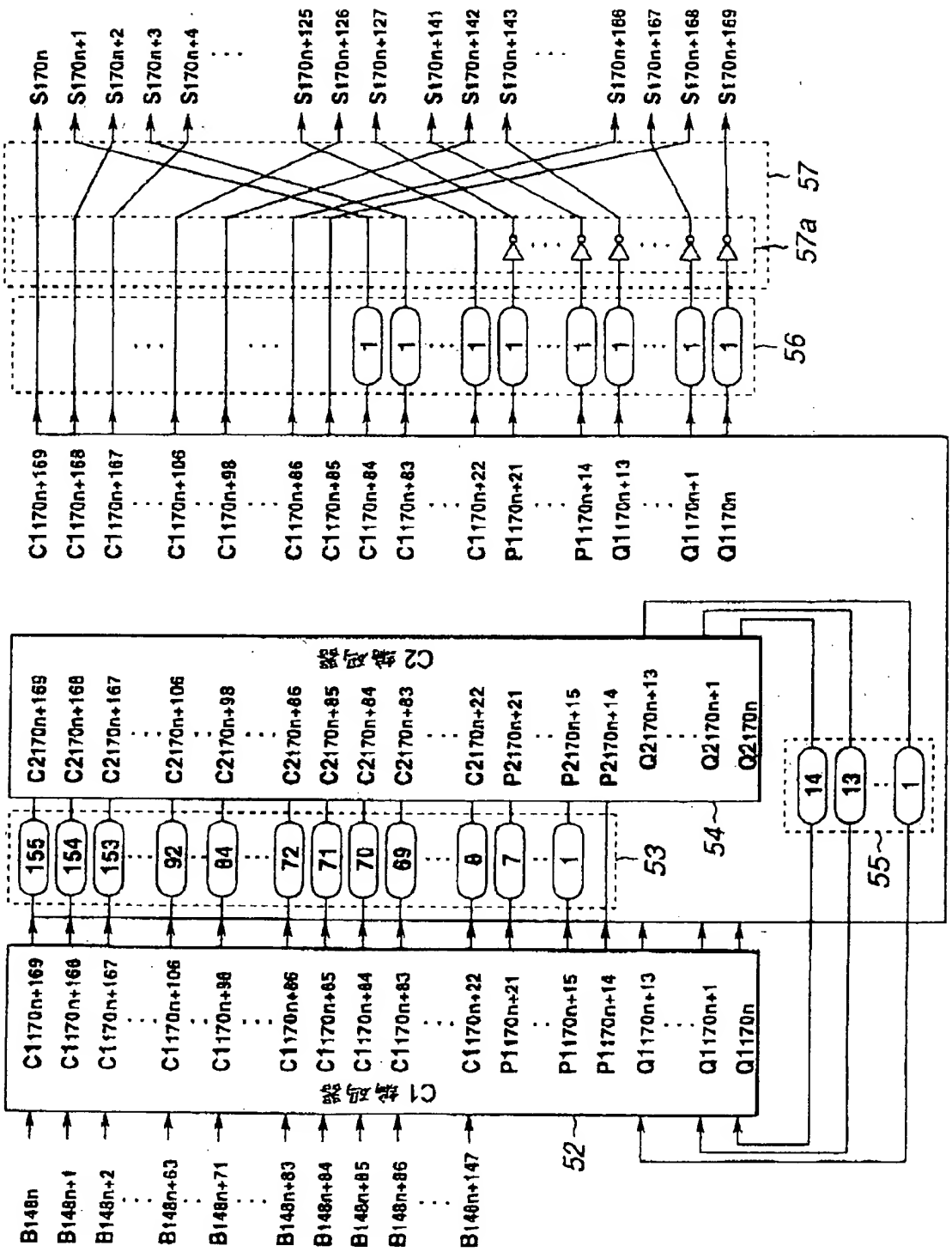

B148n
B148n+1
B148n+2
B148n+63
B148n+71
B148n+83
B148n+84
B148n+85
B148n+86
B148n+147
C1 路由器
C1170n+169
C1170n+168
C1170n+167
C1170n+106
C1170n+98
C1170n+86
C1170n+85
C1170n+84
C1170n+83
C1170n+22
P1170n+21
P1170n+15
P1170n+14
Q1170n+13
Q1170n+1
Q1170n
52
53
54
55
155
154
153
92
84
72
71
70
69
8
7
1
14
13
1
C2 路由器
C2170n+169
C2170n+168
C2170n+167
C2170n+106
C2170n+98
C2170n+86
C2170n+85
C2170n+84
C2170n+83
C2170n+22
P2170n+21
P2170n+15
P2170n+14
Q2170n+13
Q2170n+1
Q2170n
56
57a
57
S170n
S170n+1
S170n+2
S170n+3
S170n+4
S170n+125
S170n+126
S170n+127
S170n+141
S170n+142
S170n+143
S170n+166
S170n+167
S170n+168
S170n+169

图 11

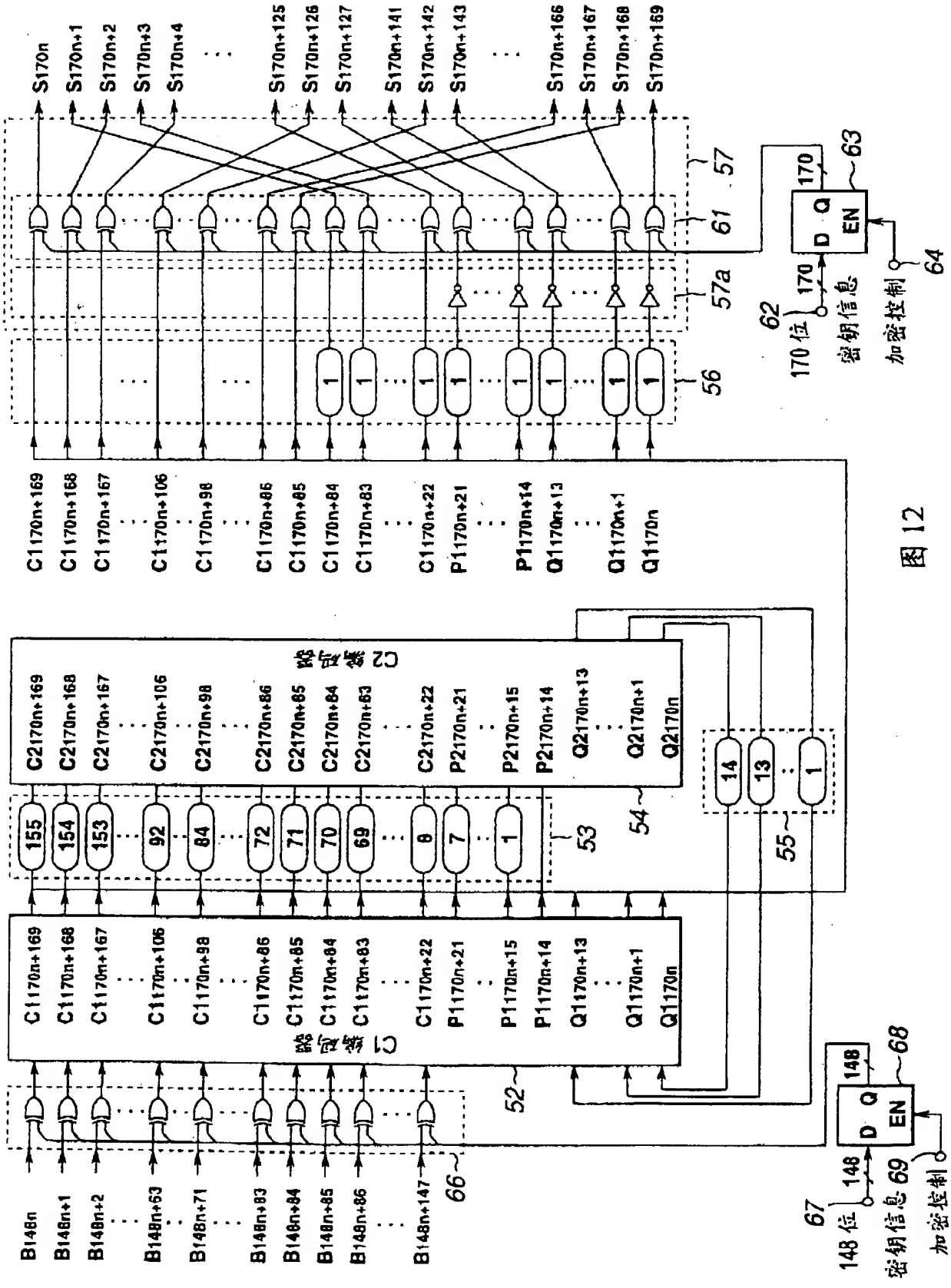

S170n
S170n+1
S170n+2
S170n+3
S170n+4
S170n+125
S170n+126
S170n+127
S170n+141
S170n+142
S170n+143
S170n+166
S170n+167
S170n+168
S170n+169
C1170n+169
C1170n+168
C1170n+167
C1170n+106
C1170n+98
C1170n+86
C1170n+85
C1170n+84
C1170n+83
C1170n+22
P1170n+21
P1170n+14
Q1170n+13
Q1170n+1
Q1170n
C2170n+169
C2170n+168
C2170n+167
C2170n+106
C2170n+98
C2170n+86
C2170n+85
C2170n+84
C2170n+83
C2170n+22
P2170n+21
P2170n+15
P2170n+14
Q2170n+13
Q2170n+1
Q2170n
B148n
B148n+1
B148n+2
B148n+63
B148n+71
B148n+83
B148n+84
B148n+85
B148n+86
B148n+147
C1 寄存器
C2 寄存器
155
154
153
92
84
72
71
70
69
0
7
1
14
13
1
52
53
54
55
56
57
57a
61
62
63
64
66
67
68
69
170
148
D Q
EN
170 位
密钥信息
加密控制
148 位
密钥信息
加密控制

图 12

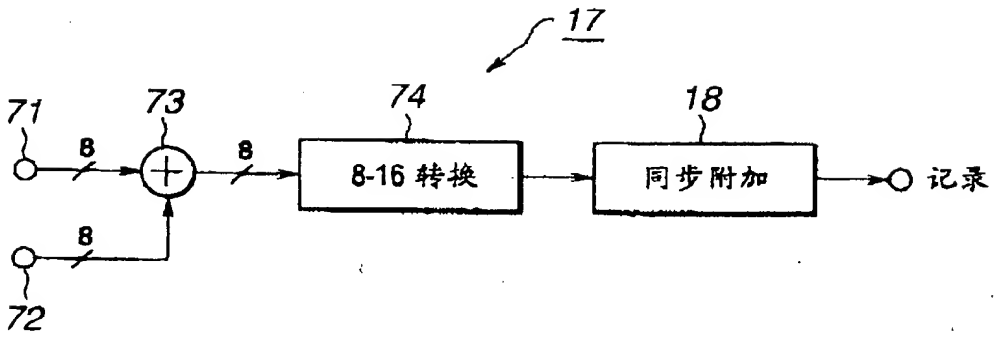


图 13

同步字	代码字	
	msb 同步模式 a lsb	msb 同步模式 b lsb
S0	00010010010000000000100000000001	10010010010000000000100000000001
S1	00010000010000000000100000000001	10010000010000000000100000000001
S2	00000100010000000000100000000001	10000100010000000000100000000001
S3	00010000010000000000100000000001	10001000010000000000100000000001

图 14

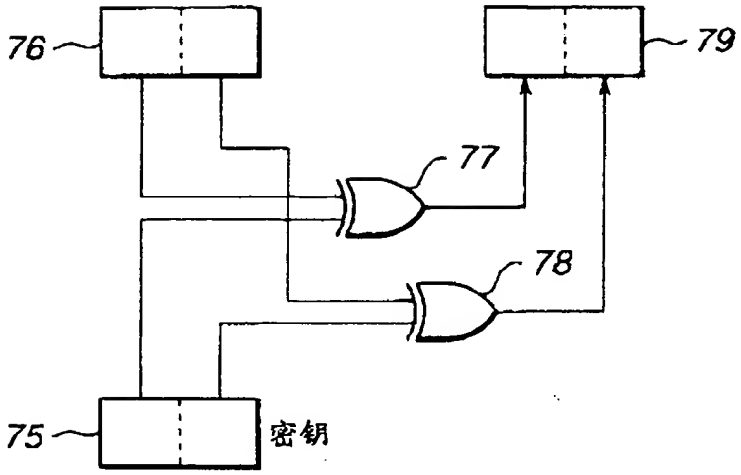


图 15

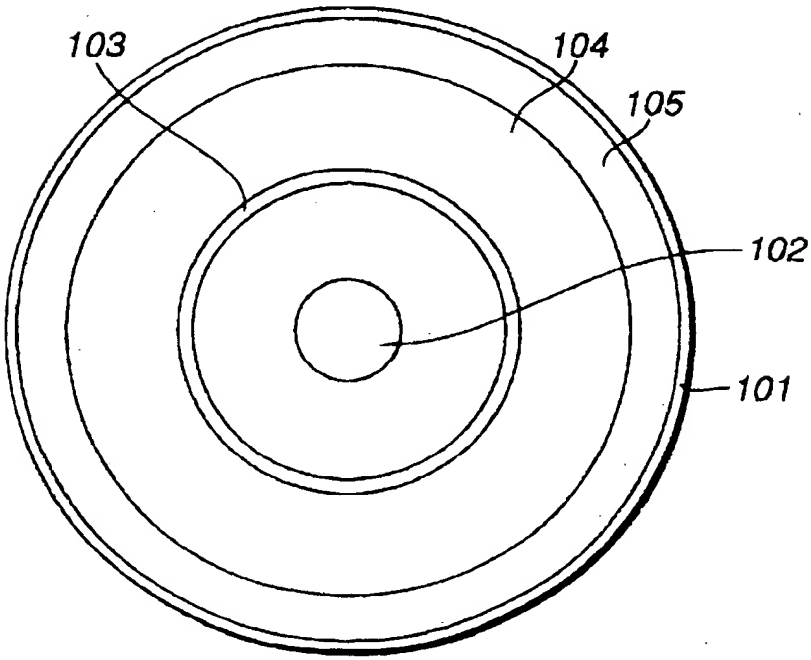


图 16

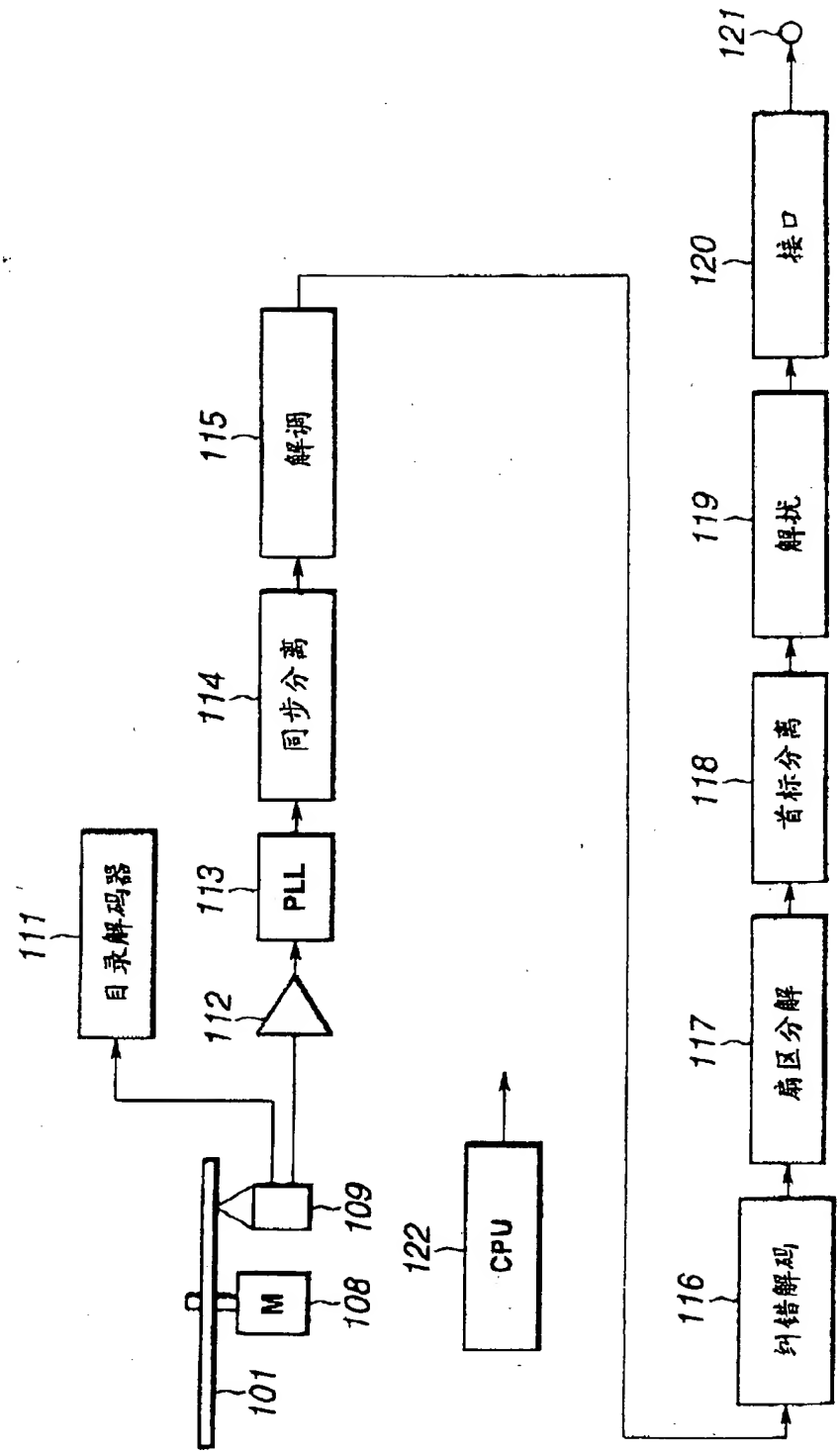

101
M
108
109
111
目录解码器
112
113
PLL
114
同步分离
115
解调
116
纠错解码
117
扇区分解
118
首标分离
119
解扰
120
接口
121
122
CPU

图 17

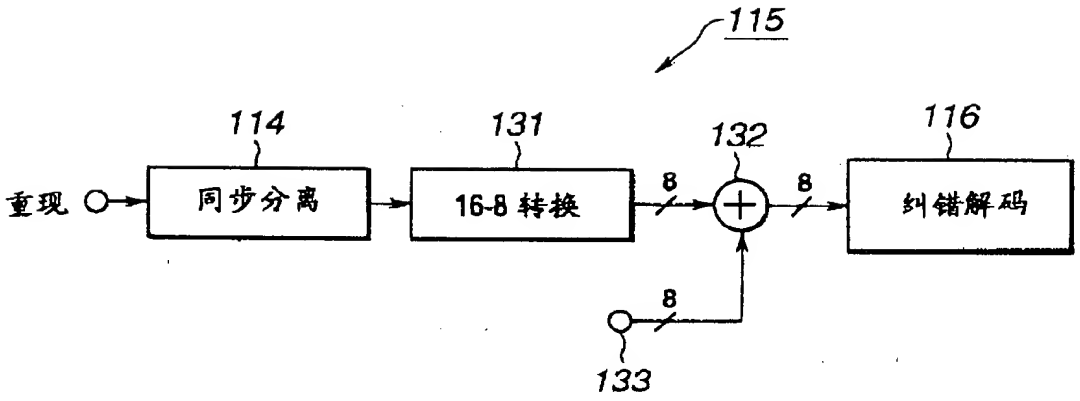


图 18

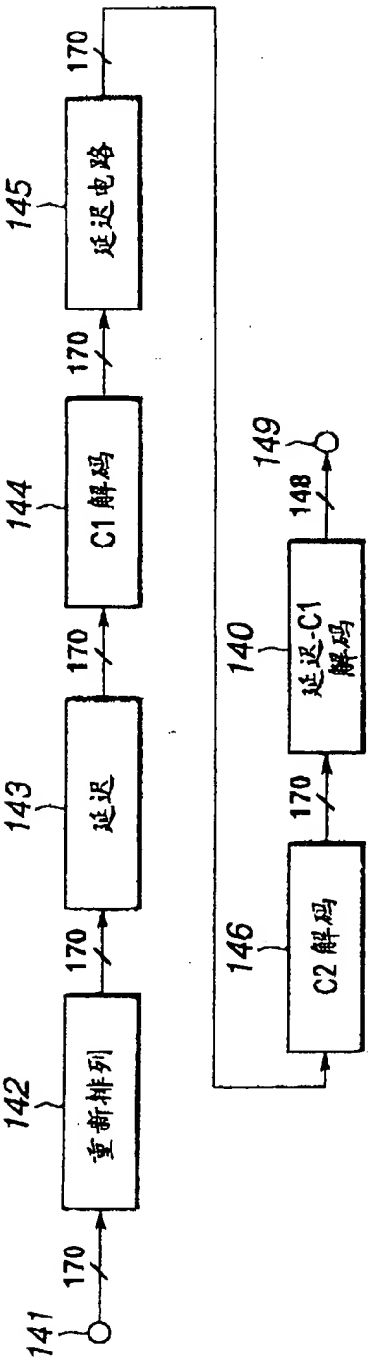

141
170
142
重新排列
170
143
延迟
170
144
C1 解码
170
145
延迟电路
170
149
148
延迟-C1
解码
140
170
146
C2 解码

图 19

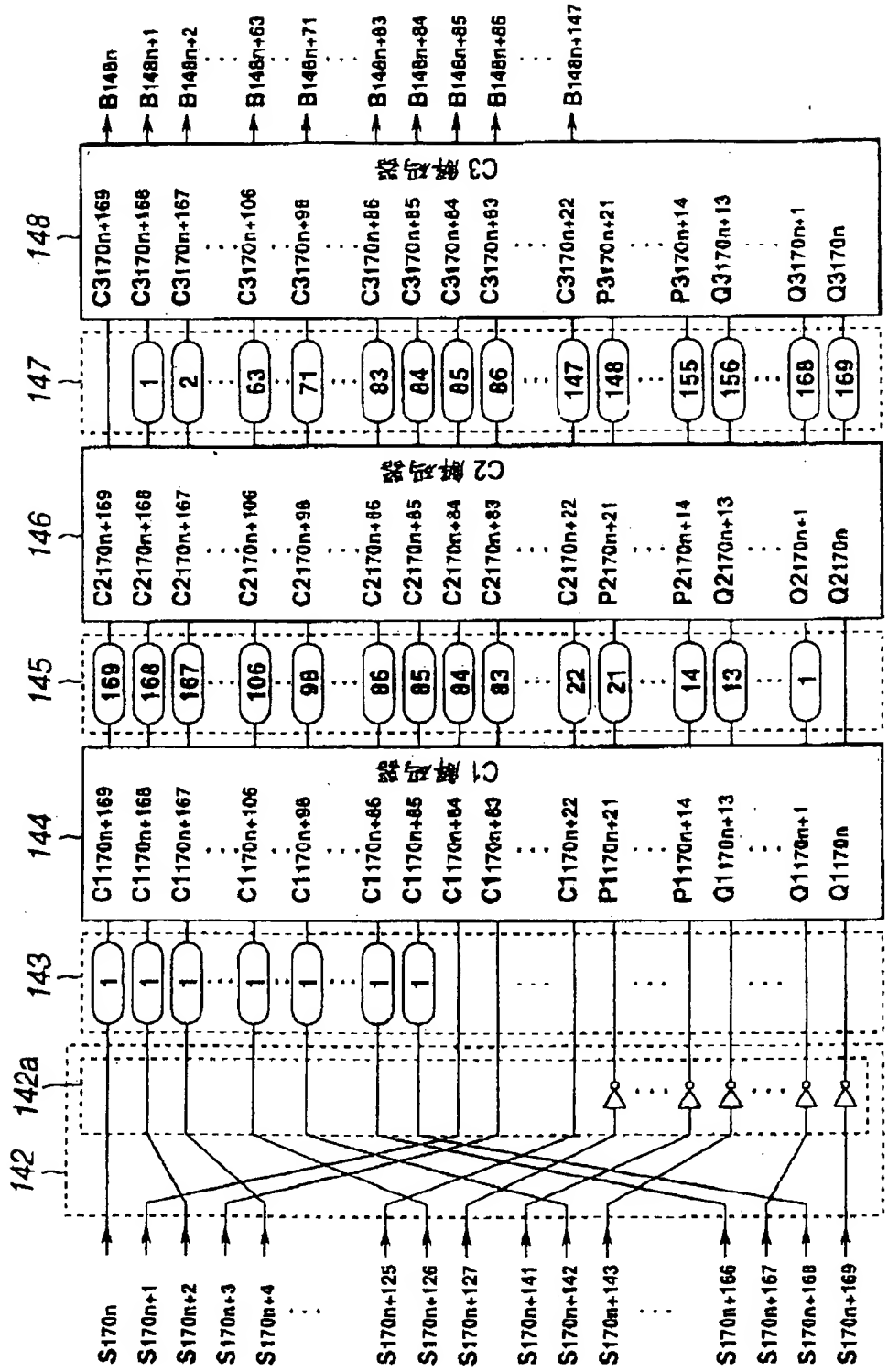

142
142a
143
144
145
146
147
148
C1 解码器
C2 解码器
C3 解码器
S170n
S170n+1
S170n+2
S170n+3
S170n+4
S170n+125
S170n+126
S170n+127
S170n+141
S170n+142
S170n+143
S170n+166
S170n+167
S170n+168
S170n+169
B148n
B148n+1
B148n+2
B148n+63
B148n+71
B148n+83
B148n+84
B148n+85
B148n+86
B148n+147

图 20

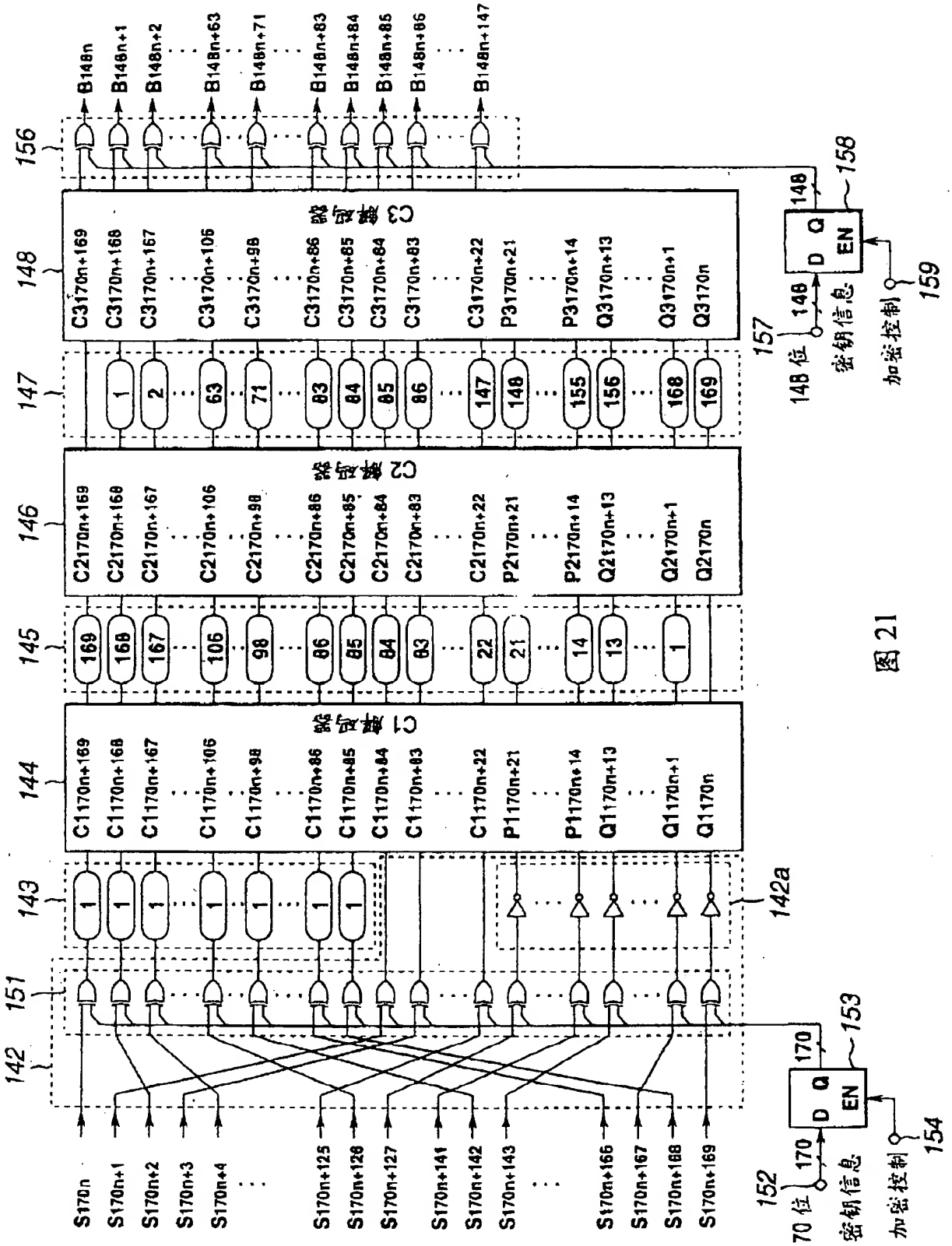

S170n
S170n+1
S170n+2
S170n+3
S170n+4
S170n+125
S170n+126
S170n+127
S170n+141
S170n+142
S170n+143
S170n+166
S170n+167
S170n+168
S170n+169
C1 累加器
C2 累加器
C3 累加器
B148n
B148n+1
B148n+2
B148n+63
B148n+71
B148n+83
B148n+84
B148n+85
B148n+86
B148n+147
170 位
148 位
密钥信息
加密控制
142
142a
143
144
145
146
147
148
151
152
153
154
156
157
158
159

图 21

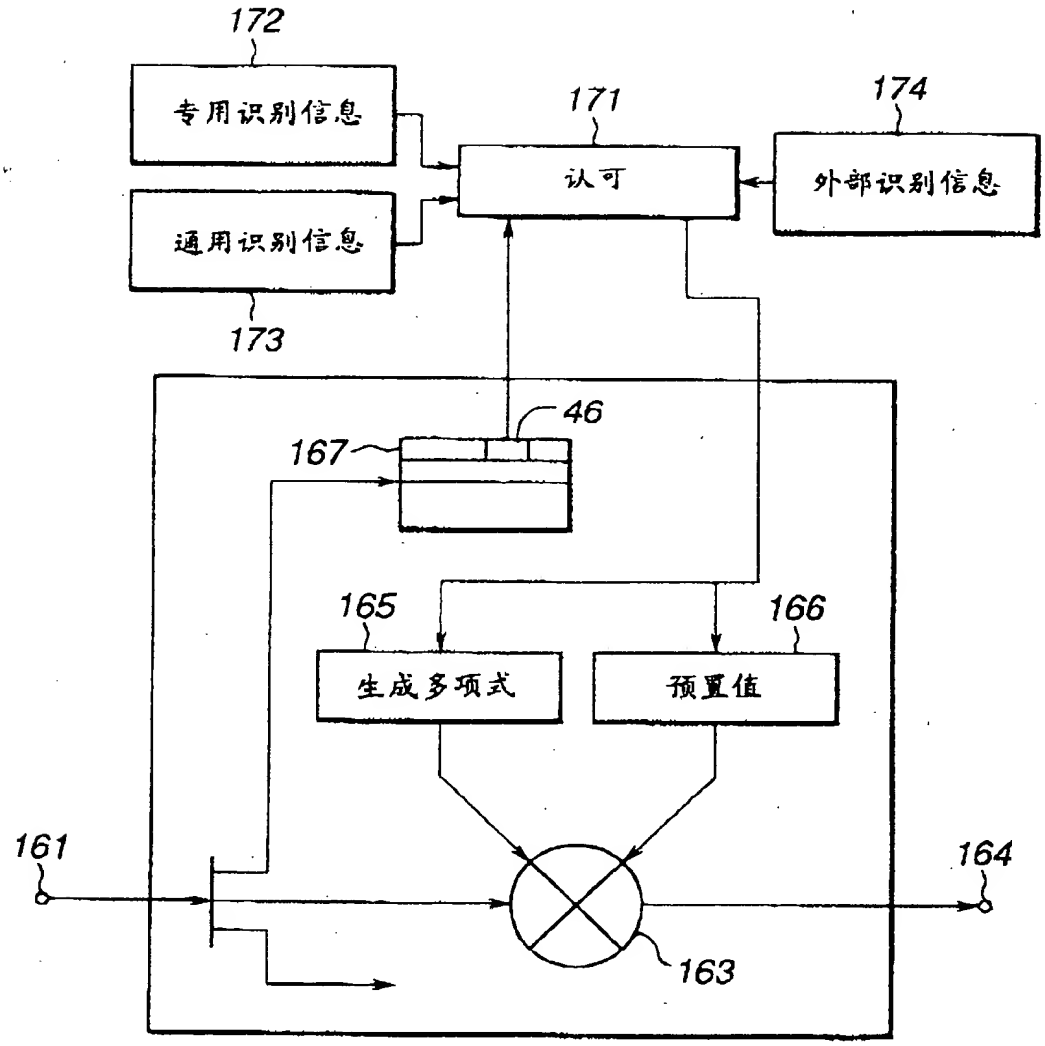

172
专用识别信息
171
认可
174
外部识别信息
通用识别信息
173
46
167
165
生成多项式
166
预置值
161
164
163

图 22

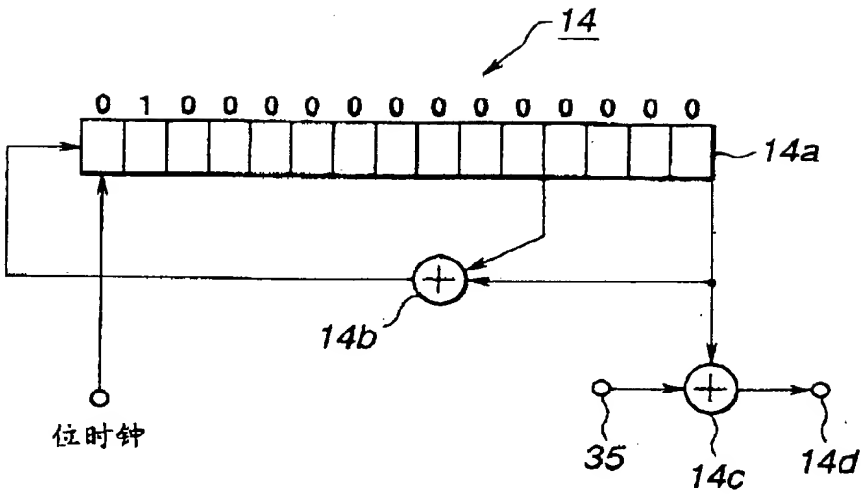


图 23

选择号	预置值	选择号	预置值
0	$0001	8	$0010
1	$5500	9	$5000
2	$0002	10	$0020
3	$2A00	11	$2001
4	$0004	12	$0040
5	$5400	13	$4002
6	$0008	14	$0080
7	$2800	15	$0005

图 24

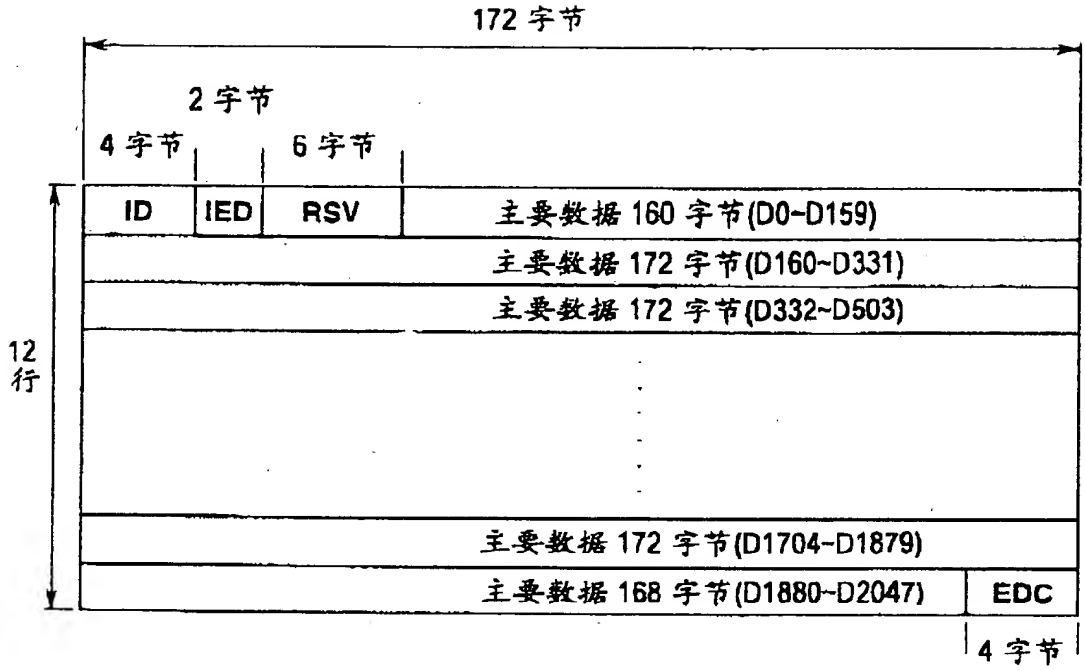

172 字节
2 字节
4 字节
6 字节
ID
IED
RSV
主要数据 160 字节(D0~D159)
主要数据 172 字节(D160~D331)
主要数据 172 字节(D332~D503)
12
行
主要数据 172 字节(D1704~D1879)
主要数据 168 字节(D1880~D2047)
EDC
4 字节

图 25

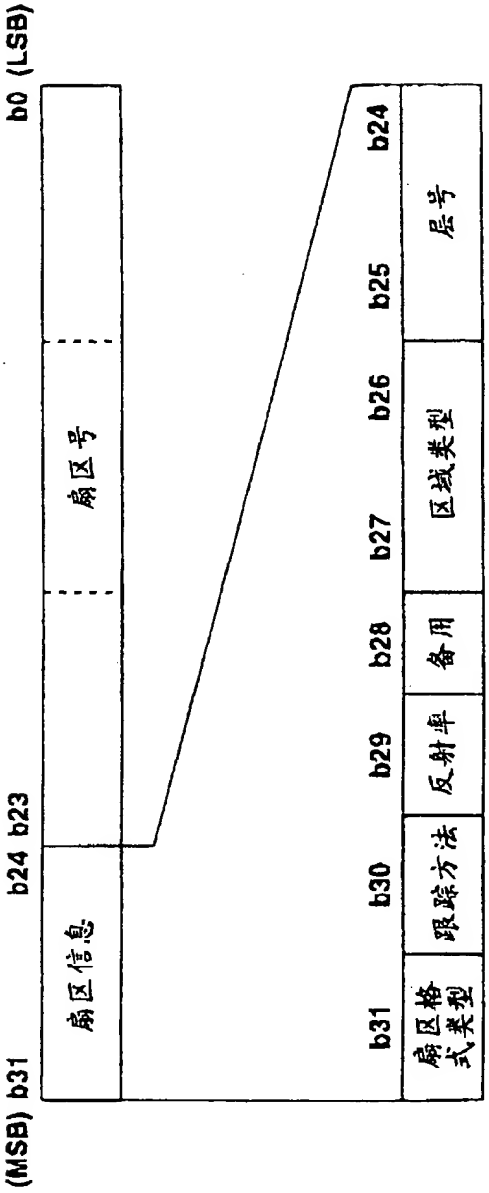

b0 (LSB)
b24 b23
(MSB) b31
扇区信息
扇区号
b31
b30
b29
b28
b27
b26
b25
b24
扇区格式类型
跟踪方法
反射率
备用
区域类型
层号

图 26

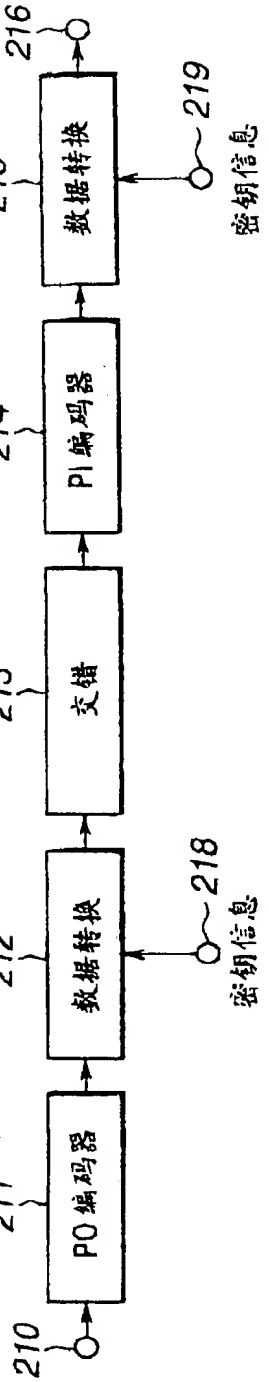

210
211
PO 编码器
212
数据转换
218
密钥信息
213
交错
214
PI 编码器
215
数据转换
219
密钥信息
216

图 27

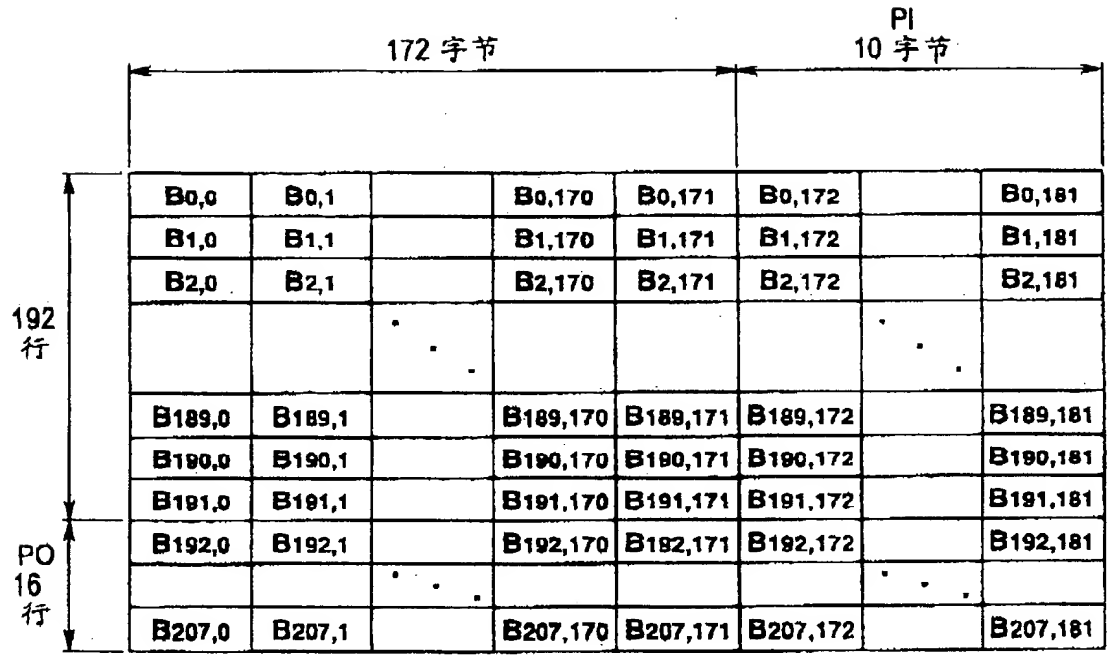

172 字节
PI
10 字节
192
行
PO
16
行
B0,0 B0,1 B0,170 B0,171 B0,172 B0,181
B1,0 B1,1 B1,170 B1,171 B1,172 B1,181
B2,0 B2,1 B2,170 B2,171 B2,172 B2,181
B189,0 B189,1 B189,170 B189,171 B189,172 B189,181
B190,0 B190,1 B190,170 B190,171 B190,172 B190,181
B191,0 B191,1 B191,170 B191,171 B191,172 B191,181
B192,0 B192,1 B192,170 B192,171 B192,172 B192,181
B207,0 B207,1 B207,170 B207,171 B207,172 B207,181

图 28

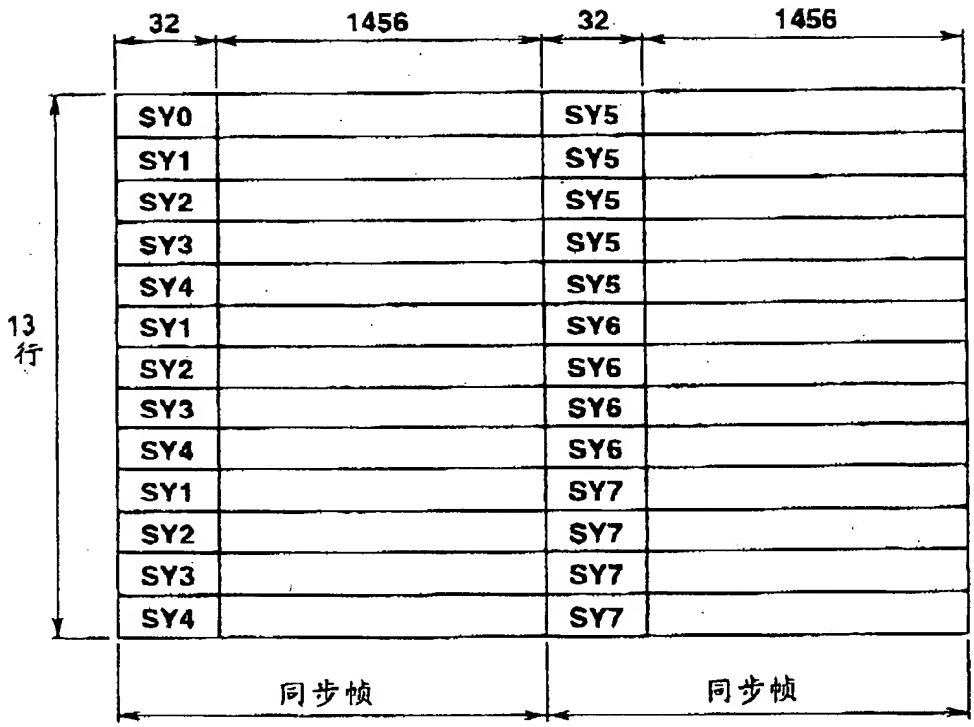

32
1456
32
1456
SY0
SY1
SY2
SY3
SY4
SY1
SY2
SY3
SY4
SY1
SY2
SY3
SY4
SY5
SY5
SY5
SY5
SY5
SY6
SY6
SY6
SY6
SY7
SY7
SY7
SY7
13
行
同步帧
同步帧

图 29

状态1和2

	(MSB)	(LSB)
SY0 =	0001001001000100	0000000000010001
SY1 =	0000100000000100	0000000000010001
SY2 =	0001000000000100	0000000001000100
SY3 =	0000100000000100	0000100000010001
SY4 =	0010000000000100	0100000000010001
SY5 =	0100010010000100	0010000100000100
SY6 =	0010010010000100	0010000010000100
SY7 =	0010010001000100	0010010000000100

图 30A

状态3和4

	(MSB)	(LSB)
SY0 =	1001001001000100	0000000000010001
SY1 =	1000010001000100	0000000000010001
SY2 =	1001000001000100	0000000000010001
SY3 =	1000001001000100	0000000000010001
SY4 =	1000100001000100	0000000000010001
SY5 =	1000010010000100	0000000000010001
SY6 =	1001000010000100	0000000000010001
SY7 =	1000010010000100	0000000000010001

图 30B

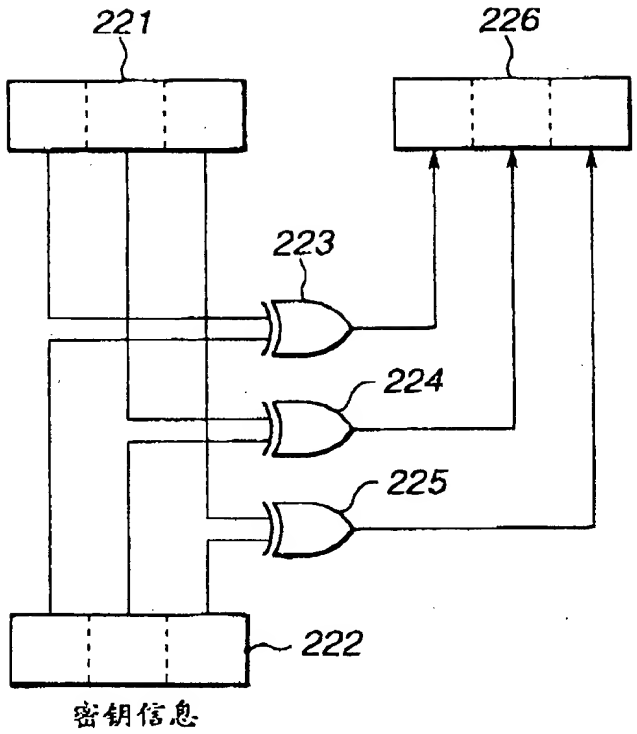


图 31

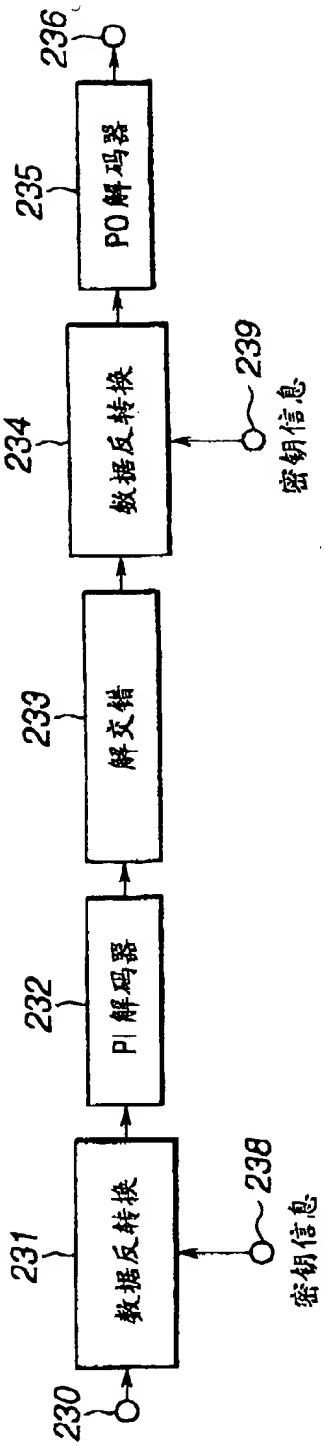

230
231
数据反转换
238
密钥信息
232
PI 解码器
233
解交错
234
数据反转换
239
密钥信息
235
PO 解码器
236

图 32